



Complete Software Guide for SRX Series Services Gateways, Release 15.1X49-D60 (Volume 1)



Modified: 2016-09-25

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Complete Software Guide for SRX Series Services Gateways, Release 15.1X49-D60 (Volume 1)
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation	lxi
Documentation and Release Notes	lxi
Using the Examples in This Manual	lxi
Merging a Full Example	lxii
Merging a Snippet	lxii
Documentation Conventions	lxiii
Documentation Feedback	lxv
Requesting Technical Support	lxv
Self-Help Online Tools and Resources	lxv
Opening a Case with JTAC	lxvi

Guide 1

Installation and Upgrade Guide

Part 1

Junos Software and Hardware Overview

Chapter 1

Software Overview	3
Junos OS Overview	3
One Operating System	4
One Modular Software Architecture	4
Junos OS Editions	5
FIPS 140-2 Security Compliance	5
Junos OS Installation Packages	6
Junos OS Package Names for EX Series Switches	7
Software Naming Convention	9
Software Naming Convention for SRX Series Devices	10
Software Package Information Security	11
Junos OS Release Numbers	11
Installation Media	12
Installation Bundles	13
Installation Modules	14
Configuration Files	15
Configuration File Selection Sequence	15
Remote Storage of Configuration Files	16
Understanding Software Infrastructure and Processes	17
Routing Engine and Packet Forwarding Engine	17
Junos OS Processes	17
Understanding Junos OS with Upgraded FreeBSD	19
Understanding Junos OS with Upgraded FreeBSD Package Names	22
Understanding Junos OS with Upgraded FreeBSD Snapshots	23
Understanding Junos OS with Upgraded FreeBSD Disk Volumes	24

Chapter 2	Hardware Overview	27
	Hardware Architecture Overview	27
	Hardware Overview (ACX Series, M Series, MX Series, T Series, and TX Matrix Routers)	28
	System Memory	29
	Storage Media	30
	Hardware Overview of SRX Series Services Gateways	31
	SRX Series Device Overview	31
	System Memory	31
	Storage Media	31
	Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)	32
	Storage Media Names for SRX Series Devices	34
	Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines	34
	Boot Sequence on SRX Series Devices	36
Part 2	Installing Junos Software	
Chapter 3	Installation Overview	41
	Installation Type Overview	41
	Standard Installation	41
	Category Change Installation	41
	Recovery Installation	42
	Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers	42
	Installation Categories on SRX Series Devices	43
	Understanding Software Installation on EX Series Switches	44
	Overview of the Software Installation Process	44
	Software Package Security	44
	Installing Software on a Virtual Chassis	45
	Installing Software on Switches with Redundant Routing Engines	45
	Installing Software Using Automatic Software Download	45
	Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick	46
	Installing Software on an EX2300 or EX3400 Switch	46
	Troubleshooting Software Installation	46
Chapter 4	Performing a Standard or Change Category Installation	47
	Checking the Current Configuration and Candidate Software Compatibility	47
	Determining the Junos OS Version	48
	Downloading Software	48
	Downloading Software with a Browser	49
	Downloading Software Using the Command-Line Interface	49
	Downloading Software Packages from Juniper Networks	51
	Understanding Download Manager for SRX Series Devices	51
	Overview	51
	Using Download Manager to Upgrade Junos OS	52
	Handling Errors	52

	Considerations	53
	Understanding the Console Port	53
	Backing Up the Existing Installation on Routers	55
	Backing Up the Current Installation on SRX Series Devices	56
	Backing Up the Current Installation on High-End SRX Series Devices	56
	Backing Up the Current Installation on Branch SRX Series Devices	57
	Installing the Software Package on a Router with a Single Routing Engine	57
	Installing the Software Package on a Router with Redundant Routing Engines	58
	Preparing the Router for the Installation	59
	Installing Software on the Backup Routing Engine	59
	Installing Software on the Master Routing Engine	61
	Finalizing the Installation	63
	Repartitioning Routing Engine System Storage To Increase the Swap Partition	64
	Installing Software on EX Series Switches (J-Web Procedure)	64
	Installing Software Upgrades from a Server	65
	Installing Software Upgrades by Uploading Files	65
	Registering the EX Series Switch with the J-Web Interface	66
	Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices	66
	Installing Junos OS on SRX Series Devices Using a USB Flash Drive	68
	Upgrading the Boot Loader on SRX Series Devices	69
	Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server	70
	Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device	72
Chapter 5	Configuring Zero Touch Provisioning	73
	Understanding Zero Touch Provisioning	73
	Configuring Zero Touch Provisioning	76
Chapter 6	Configuring Automatic Installation of Configuration Files	81
	Autoinstallation Overview	81
	Automatic Installation of Configuration Files	82
	Supported Autoinstallation Interfaces and Protocols	82
	Typical Autoinstallation Process on a New Device	83
	Configuring Autoinstallation on SRX Series Devices	84
	Configuring Autoinstallation on JNU Satellite Devices	87
	Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group	89
	Supported Autoinstallation Interfaces and Protocols	89
	Typical Autoinstallation Process on a New Router	90
	Autoinstallation of Satellite Devices in a Junos Node Unifier Group	91
	Verifying Autoinstallation on JNU Satellite Devices	92
Chapter 7	Configuring Dual-Root Partitions for High Availability	95
	Understanding Resilient Dual-Root Partitions on Switches	95
	Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)	96
	Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature	96

Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)	97
Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases	98
Resilient Dual-Root Partitions Frequently Asked Questions	99
How Does Upgrading to Junos OS Release 10.4R3 and Later Differ from Normal Upgrades?	99
What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time?	100
Can I Downgrade Junos OS Without Downgrading the Loader Software?	101
Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI?	101
Will I Lose My Configuration During an Upgrade?	102
How Long Will the Upgrade Process Take?	102
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Enabled?	102
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Not Enabled?	103
How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System?	103
Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release?	104
Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch?	104
Where Can I Find Instructions for Upgrading?	104
Dual-Root Partitioning Scheme on SRX Series Devices	105
Boot Media and Boot Partition on SRX Series Devices	106
Important Features of the Dual-Root Partitioning Scheme	106
Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning	106
Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices	108
Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning	109
Example: Installing Junos OS on SRX Series Devices Using the Partition Option	110
Chapter 8 Upgrading Software	115
Upgrading Software Packages	116
Upgrading to 64-bit Junos OS	119
Upgrading Routers Using Unified ISSU	122
Understanding Nonstop Software Upgrade on EX Series Switches	123
Requirements for Performing an NSSU	124
How an NSSU Works	125
EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis	125
EX6200 and EX8200 Switches	126
EX8200 Virtual Chassis	127
NSSU Limitations	128
NSSU and Junos OS Release Support	128

Overview of NSSU Configuration and Operation	129
Upgrading Software by Using Automatic Software Download	129
Verifying That Automatic Software Download Is Working Correctly	131
Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch	131
Verifying the Number of Partitions and File System Mountings	132
Verifying the Loader Software Version	132
Verifying Which Root Partition Is Active	133
Verifying the Junos OS Version in Each Root Partition	134
Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis	136
Upgrading Junos OS with Upgraded FreeBSD	139
To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS	141
To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release	144
To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release	145
Understanding Junos OS Upgrades for SRX Series Devices	145
Understanding Junos OS Upgrades	146
Junos OS Upgrade Methods on the SRX Series Devices	146
Preparing Your SRX Series Device for Junos OS Upgrades	147
Secondary Storage Devices Available on SRX Series Devices	147
Verifying Available Disk Space on SRX Series Devices	148
Cleaning Up the System File Storage Space	149
Downloading Software Packages from Juniper Networks	150
Example: Installing Junos OS Upgrade Packages on SRX Series Devices	150
Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server	152
Understanding BIOS Upgrades on SRX Series Devices	154
Understanding Manual BIOS Upgrade Using the Junos CLI	154
Understanding Auto BIOS Upgrade Methods on SRX Series Devices	155
Disabling Auto BIOS Upgrade on SRX Series Devices	155
Example: Downgrading Junos OS on SRX Series Devices	156
Chapter 9 Booting a Device Using a System Snapshot	159
Understanding System Snapshot on EX Series Switches	159
Creating a Snapshot and Using It to Boot an EX Series Switch	160
Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch	160
Verifying That a System Snapshot Was Created on an EX Series Switch	161
Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive	162

Chapter 10	Performing a Recovery Installation	165
	Creating an Emergency Boot Device	165
	Configuring Boot Devices for SRX Series Devices	166
	Example: Creating a Snapshot and Using It to Boot an SRX Series Device	166
	Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices	169
	Overview	169
	How Autorecovery Works	170
	How to Use Autorecovery	170
	Data That Is Backed Up in an Autorecovery	170
	Troubleshooting Alarms	171
	Considerations	171
	Performing a Recovery Installation	172
	Creating a New Configuration on a Single Routing Engine	173
	Log In to the Router Console	173
	Configure Administration User Accounts	174
	Add the Management Console to the Network	174
	Commit Changes	175
	Creating a New Configuration with Redundant Routing Engines	177
	Configure Administration User Accounts	178
	Set Up Routing Engine Configuration Groups	178
	Complete the Management Console Configuration	180
	Commit and Synchronize Changes	181
	Saving a Rescue Configuration File	183
	Restoring a Saved Configuration	184
	Copy Saved Files to the Router	184
	Loading and Committing the Configuration File	184
	Reverting to the Default Factory Configuration by Using the request system zeroize Command	185
	Reverting to the Rescue Configuration	186
Chapter 11	Reinstalling Software	187
	Checklist for Reinstalling Junos OS	187
	Log the Software Version Information	189
	Log the Hardware Version Information	190
	Log the Chassis Environment Information	191
	Log the System Boot-Message Information	192
	Log the Active Configuration	194
	Log the Interfaces on the Router	194
	Log the BGP, IS-IS, and OSPF Adjacency Information	195
	Log the System Storage Information	196
	Back Up the Currently Running and Active File System	197

	Reinstall Junos OS	197
	Reconfigure Junos OS	198
	Configure Host Names, Domain Names, and IP Addresses	198
	Protecting Network Security by Configuring the Root Password	200
	Check Network Connectivity	201
	Copy Backup Configurations to the Router	202
	Configure Host Names, Domain Names, and IP Addresses	202
	Protecting Network Security by Configuring the Root Password	204
	Check Network Connectivity	206
	Copy Backup Configurations to the Router	206
	After You Reinstall Junos OS	206
	Compare Information Logged Before and After the Reinstall	206
	Back Up the New Software	207
	Compare Information Logged Before and After the Reinstall	207
	Back Up the New Software	207
Chapter 12	Downgrading Software	209
	Downgrading Junos OS from Upgraded FreeBSD	209
	Downgrading from Junos OS with Upgraded FreeBSD to Junos OS	209
	Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD	211
Chapter 13	Rebooting or Halting Software Processes on a Device	213
	Restarting and Halting SRX Series Devices	213
	Rebooting SRX Series Devices	213
	Halting SRX Series Devices	215
	Bringing Chassis Components Online and Offline on SRX Series Devices	217
	Restarting the Chassis on SRX Series Devices	217
	Bringing Chassis Components Online and Offline on SRX Series Devices	218
	Restarting the Chassis on SRX Series Devices	218
	Rebooting or Halting the EX Series Switch (J-Web Procedure)	219
Part 3	Installing and Managing Software Licenses	
Chapter 14	Software License Overview	223
	Junos OS Feature Licenses	223
	License Enforcement	224
	Junos OS Feature License Keys	225
	Release-Tied License Keys and Upgrade Licenses on MX Series Routers	225
	Licensable Ports on MX5, MX10, and MX40 Routers	226
	Port Activation on MX104 Routers	227
	Software Feature Licenses	228
	Software Features That Require Licenses on M Series, MX Series, and T Series Routers	228
	Software Features That Require Licenses on M Series Routers Only	231
	Software Features That Require Licenses on MX Series Routers Only	232
	Software Feature Licenses for SRX Series Devices	236
	Software Features That Require Licenses on EX Series Switches	241
	Software Features That Require Licenses on the QFX Series	243

	Understanding Software Licenses for EX Series Switches	246
	Purchasing a Software Feature License	246
	Features Requiring a License on EX2200 Switches	247
	Features Requiring a License on EX2300 Switches	248
	Features Requiring a License on EX3300 Switches	248
	Features Requiring a License on EX3400 Switches	249
	Features Requiring a License on EX4300 Switches	250
	Features Requiring a License on EX4600 Switches	252
	Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches	253
	License Warning Messages	254
Chapter 15	Installing and Managing Licenses	257
	Adding New Licenses (CLI Procedure)	257
	Deleting a License (CLI Procedure)	258
	Saving License Keys	259
	Verifying Junos OS License Installation	260
	Displaying Installed Licenses	260
	Displaying License Usage	261
Part 4	Troubleshooting Information	
Chapter 16	Troubleshooting Software Installation	265
	Troubleshooting Software Installation	265
	Recovering from a Failed Software Upgrade on an EX Series Switch	265
	Rebooting from the Inactive Partition	266
	Freeing Disk Space for Software Installation	267
	Installation from the Boot Loader Generates 'cannot open package' Error	267
	Troubleshooting a Switch That Has Booted from the Backup Junos OS Image	268
	Disk Space Management for Junos OS Installation	269
	Verifying PIC Combinations	269
Part 5	Configuration Statements and Operational Commands	
Chapter 17	Configuration Statements	273
	auto-configuration	274
	auto-configuration (System)	275
	auto-image-upgrade	277
	auto-snapshot	278
	autoinstallation	279
	autoinstallation (JNU Satellite Devices)	280
	bootp	281
	commit	282
	configuration-servers	283
	delete-after-commit (JNU Satellites)	284
	interfaces (Autoinstallation)	285
	license	286
	usb	288

Chapter 18

usb-control	288
Operational Commands	289
clear system login lockout	291
request system autorecovery state	292
request system download abort	294
request system download clear	295
request system download pause	296
request system download resume	297
request system download start	298
request system firmware upgrade	299
request system halt	300
request system license add	302
request system license delete	303
request system license save	304
request system license update	305
request system partition compact-flash	306
request system power-off	307
request system reboot	309
request system reboot	314
request system reboot (Junos OS with Upgraded FreeBSD)	316
request system scripts add	319
request system scripts delete	320
request system scripts rollback	321
request system snapshot	322
request system snapshot (Junos OS with Upgraded FreeBSD)	329
request system snapshot (SRX Series)	331
request system software abort in-service-upgrade (ICU)	333
request system software add	334
request system software add (Maintenance)	344
request system software configuration-backup	345
request system software configuration-restore	346
request system software delete	347
request system software rollback	351
request system software rollback (SRX Series)	356
request system software validate	357
request system software validate on (Junos OS with Upgraded FreeBSD)	361
request system storage cleanup	364
request system storage cleanup (SRX Series)	374
request system zeroize	377
show chassis usb storage	382
show system autoinstallation status	383
show system autorecovery state	385
show system boot-messages	387
show system auto-snapshot	394
show system download	396
show system license	398
show system license (View)	406
show system login lockout	409

show system snapshot	410
show system snapshot (Junos OS with Upgraded FreeBSD)	413
show system snapshot media	414
show system storage partitions (EX Series Switches Only)	415
show system storage partitions (View SRX Series)	417

Guide 2 CLI User Guide

Chapter 19	Overview	421
	Introducing the Junos OS Command-Line Interface	421
	Key Features of the CLI	422
	Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies	423
	Junos OS CLI Command Modes	423
	CLI Command Hierarchy	424
	Configuration Statement Hierarchy	424
	Moving Among Hierarchy Levels	425
	Other Tools to Configure and Monitor Devices Running Junos OS	426
	Commands and Configuration Statements for Junos-FIPS	426
Chapter 20	Getting Started: A Quick Tour of the CLI	429
	Getting Started with the Junos OS Command-Line Interface	429
	Switching Between Junos OS CLI Operational and Configuration Modes	431
	Configuring a User Account on a Device Running Junos OS	432
	Using the CLI Editor in Configuration Mode	434
	Checking the Status of a Device Running Junos OS	436
	Example: Configuring a Routing Protocol	438
	Shortcut	439
	Longer Configuration	439
	Making Changes to a Routing Protocol Configuration	441
	Rolling Back Junos OS Configuration Changes	444
Chapter 21	Getting Online Help	447
	Getting Online Help from the Junos OS Command-Line Interface	447
	Getting Help About Commands	447
	Getting Help About a String in a Statement or Command	448
	Getting Help About Configuration Statements	449
	Getting Help About System Log Messages	449
	Junos OS CLI Online Help Features	450
	Help for Omitted Statements	450
	Using CLI Command Completion	450
	Using Command Completion in Configuration Mode	451
	Displaying Tips About CLI Commands	451
	Examples: Using Command Completion in Configuration Mode	451
	Examples: Using the Junos OS CLI Command Completion	453
	Displaying the Junos OS CLI Command and Word History	454

Chapter 22	Using Configuration Statements to Configure a Device	455
	Understanding Junos OS CLI Configuration Mode	456
	Configuration Mode Commands	457
	Configuration Statements and Identifiers	458
	Configuration Statement Hierarchy	460
	Entering and Exiting the Junos OS CLI Configuration Mode	462
	Notational Conventions Used in Junos OS Configuration Hierarchies	464
	Forms of the configure Command	465
	Using the configure exclusive Command	467
	Using the configure Command	468
	Modifying the Junos OS Configuration	468
	Adding Junos OS Configuration Statements and Identifiers	469
	Deleting a Statement from a Junos OS Configuration	470
	Example: Deleting a Statement from the Junos OS Configuration	471
	Copying a Junos OS Statement in the Configuration	473
	Example: Copying a Statement in the Junos Configuration	473
	Issuing Relative Junos OS Configuration Mode Commands	475
	Renaming an Identifier in a Junos OS Configuration	476
	Examples: Re-Using Configuration	476
	Inserting a New Identifier in a Junos OS Configuration	481
	Example: Inserting a New Identifier in a Junos Configuration	481
	Example: Using the Wildcard Command with the Range Option	485
	Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration	489
	Example: Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration	490
	Adding Comments in a Junos OS Configuration	492
	Adding Comments in the CLI	492
	Adding Comments in a File	493
	Example: Including Comments in a Junos OS Configuration by Using the CLI	494
	Updating the configure private Configuration	496
	Displaying the Current Junos OS Configuration	497
	Example: Displaying the Current Junos OS Configuration	498
	Displaying Additional Information About the Junos OS Configuration	499
	Displaying set Commands from the Junos OS Configuration	501
	Example: Displaying set Commands from the Configuration	502
	Example: Displaying Required set Commands at the Current Hierarchy Level	502
	Example: Displaying set Commands with the match Option	503
	Displaying Users Currently Editing the Junos OS Configuration	504
	Verifying a Junos OS Configuration	504
Chapter 23	Committing a Junos OS Configuration	507
	Junos OS Commit Model for Router or Switch Configuration	507
	Committing a Junos OS Configuration	508
	Committing a Junos OS Configuration and Exiting Configuration Mode	510
	Commit Operation When Multiple Users Configure the Software	511
	Activating a Junos OS Configuration but Requiring Confirmation	512
	Scheduling a Junos OS Commit Operation	513

	Monitoring the Junos OS Commit Process	514
	Adding a Comment to Describe the Committed Configuration	515
	Backing Up the Committed Configuration on the Alternate Boot Drive	516
	Junos OS Batch Commits Overview	516
	Aggregation and Error Handling	517
	Example: Configuring Batch Commit Server Properties	517
Chapter 24	Managing Configurations	525
	Understanding How the Junos OS Configuration Is Stored	525
	Comparing Configuration Changes with a Prior Version	526
	Understanding the show compare display xml Command Output	528
	Adding a Statement (create Operation)	529
	Deleting a Statement (delete Operation)	529
	Changing a Statement (delete and create Operations)	530
	Changing Metadata (inactive Attribute and Operation)	531
	Adding an Annotation (comment Tag and create Operation)	532
	Changing an Annotation (comment Tag, and delete and create Operations)	532
	Adding a Statement Inside a Container (create Operation, and insert and key Attributes)	533
	Changing the Order Inside a Container (merge Operation, and insert and key Attributes)	534
	Returning to the Most Recently Committed Junos OS Configuration	534
	Returning to a Previously Committed Junos OS Configuration	535
	Returning to a Configuration Prior to the One Most Recently Committed	535
	Displaying Previous Configurations	535
	Comparing Configuration Changes with a Prior Version	536
	Creating and Returning to a Rescue Configuration	538
	Saving a Configuration to a File	539
	Saving a Configuration to a File	540
	Additional Details About Specifying Junos OS Statements and Identifiers	541
	Specifying Statements	541
	Performing CLI Type Checking	543
	Loading a Configuration from a File	544
	Examples: Loading a Configuration from a File	547
	Creating and Returning to a Rescue Configuration	549
	Compressing the Current Configuration File	549
	Example: Protecting the Junos OS Configuration from Modification or Deletion	551
	Synchronizing Routing Engines	558
	Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically	560
Chapter 25	Using Operational Commands to Monitor a Device	563
	Overview of Junos OS CLI Operational Mode Commands	563
	CLI Command Categories	563
	Commonly Used Operational Mode Commands	565
	Junos OS Operational Mode Commands That Combine Other Commands	566
	Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands	567

Controlling the Scope of an Operational Mode Command	568
Operational Mode Commands on a TX Matrix Router or TX Matrix Plus Router	569
Examples of Routing Matrix Command Options	569
Monitoring Who Uses the Junos OS CLI	571
Interface Naming Conventions Used in the Junos OS Operational Commands	572
Physical Part of an Interface Name	572
Logical Part of an Interface Name	572
Channel Identifier Part of an Interface Name	573
Viewing Files and Directories on a Device Running Junos OS	573
Directories on the Router or Switch	573
Listing Files and Directories	574
Specifying Filenames and URLs	576
Displaying Junos OS Information	577
Managing Programs and Processes Using Junos OS Operational Mode Commands	579
Showing Software Processes	580
Restarting the Junos OS Process	581
Stopping Junos OS	582
Rebooting Junos OS	583
Using the Junos OS CLI Comment Character # for Operational Mode Commands	584
Example: Using Comments in Junos OS Operational Mode Commands	584
Chapter 26 Filtering Command Output	587
Using the Pipe () Symbol to Filter Junos OS Command Output	587
Using Regular Expressions with the Pipe () Symbol to Filter Junos OS Command Output	588
Filtering Operational Mode Command Output in a QFabric System	589
Pipe () Filter Functions in the Junos OS Command-Line Interface	590
Comparing Configurations and Displaying the Differences in Text	590
Comparing Configurations and Displaying the Differences in XML	592
Counting the Number of Lines of Output	592
Displaying Output in XML Tag Format	592
Displaying Output in JSON Format	593
Displaying the RPC tags for a Command	593
Ignoring Output That Does Not Match a Regular Expression	593
Displaying Output from the First Match of a Regular Expression	594
Retaining Output After the Last Screen	594
Displaying Output Beginning with the Last Entries	594
Displaying Output That Matches a Regular Expression	595
Preventing Output from Being Paginated	595
Sending Command Output to Other Users	595
Resolving IP Addresses	596
Saving Output to a File	596
Appending Output to a File	596
Displaying Output on Screen and Writing to a File	597
Trimming Output by Specifying the Starting Column	597

	Refreshing the Output of a Command	597
Chapter 27	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	599
	Using Keyboard Sequences to Move Around and Edit the Junos OS CLI	599
	Using Wildcard Characters in Interface Names	601
	Common Regular Expressions to Use with the replace Command	602
	Using Global Replace in the Junos OS Configuration	603
	Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference	604
	Example: Using Global Replace in a Junos OS Configuration—Replacing an Interface Name	606
	Example: Using Global Replace in a Junos OS Configuration—Using the upto Option	608
	Using Regular Expressions to Delete Related Items from a Junos OS cConfiguration	609
Chapter 28	Using Configuration Groups to Quickly Configure Devices	613
	Understanding Junos OS Configuration Groups	614
	Configuration Groups Overview	614
	Inheritance Model	614
	Configuring Configuration Groups	614
	Creating the Junos OS Configuration Group	615
	Applying the Junos OS Configuration Group	617
	Example: Configuring and Applying Junos OS Configuration Groups	618
	Example: Creating and Applying Configuration Groups on a TX Matrix Router	619
	Disabling Inheritance of a Junos OS Configuration Group	620
	Using Wildcards with Configuration Groups	622
	Example: Configuring Sets of Statements with Configuration Groups	625
	Example: Configuring Interfaces Using Junos OS Configuration Groups	626
	Example: Configuring a Consistent IP Address for the Management Interface	628
	Example: Configuring Peer Entities	630
	Establishing Regional Configurations	631
	Configuring Wildcard Configuration Group Names	633
	Example: Referencing the Preset Statement From the Junos OS defaults Group	634
	Example: Viewing Default Statements That Have Been Applied to the Configuration	635
	Using Conditions to Apply Configuration Groups Overview	636
	Example: Configuring Conditions for Applying Configuration Groups	636
	Improving Commit Time When Using Configuration Groups	638
	Example: Improving Commit Time When Using Configuration Groups	639
	Using Junos OS Defaults Groups	640
	Set Up Routing Engine Configuration Groups	642
Chapter 29	Controlling the CLI Environment	645
	Controlling the Junos OS CLI Environment	645
	Setting the Terminal Type	646
	Setting the CLI Prompt	646
	Setting the CLI Directory	646
	Setting the CLI Timestamp	646

	Setting the Idle Timeout	646
	Setting the CLI to Prompt After a Software Upgrade	646
	Setting Command Completion	647
	Displaying CLI Settings	647
	Setting the Junos OS CLI Screen Length and Width	647
	Setting the Screen Length	647
	Setting the Screen Width	648
	Example: Controlling the CLI Environment	648
	Example: Enabling Configuration Breadcrumbs	654
Chapter 30	Junos OS Configuration Statements and Commands	657
	apply-groups	658
	apply-groups-except	659
	activate	660
	annotate	661
	commit	662
	commit-interval (Batch Commits)	667
	configuration-breadcrumbs	668
	copy	669
	days-to-keep-error-logs (Batch Commits)	669
	deactivate	670
	delete	671
	edit	672
	exit	673
	groups	674
	help	676
	insert	677
	load	678
	maximum-aggregate-pool (Batch Commits)	679
	maximum-entries (Batch Commits)	680
	protect	681
	quit	682
	rename	683
	replace	684
	rollback	685
	run	686
	save	687
	server (Batch Commits)	688
	set	689
	show	690
	show configuration	691
	show display inheritance	694
	show display omit	695
	show display set	696
	show display set relative	697
	show groups junos-defaults	698
	status	699
	top	700
	traceoptions (Batch Commits)	701

	unprotect	702
	up	703
	update	704
	when	705
	wildcard delete	707
Chapter 31	Junos OS CLI Environment Commands	709
	set cli complete-on-space	710
	set cli directory	711
	set cli idle-timeout	712
	set cli prompt	713
	set cli restart-on-upgrade	714
	set cli screen-length	715
	set cli screen-width	716
	set cli terminal	717
	set cli timestamp	718
	set date	719
	show cli	720
	show cli	722
	show cli authorization	723
	show cli directory	724
	show cli history	725
Chapter 32	Junos OS CLI Operational Mode Commands	727
	configure	728
	file	730
	help	731
	(pipe)	732
	request	735
	request system commit server pause	737
	request system commit server queue cleanup	738
	request system commit server start	739
	restart	740
	set	751
	show system commit server queue	752
	show system commit server status	756
Guide 3	J-Web User Guide for Security Devices	
Part 6	Overview	
Chapter 33	Understanding the J-Web User Interface	761
	J-Web Overview	761
	Starting the J-Web User Interface	762
	Understanding the J-Web Interface Layout	762
	Top Pane	763
	Main Pane	764
	Side Pane	764
	Getting Help in the J-Web User Interface	765

Part 7	Configuring and Managing a Device Using J-Web	
Chapter 34	Installing J-Web	769
	J-Web Software Requirements	769
	Installing the J-Web Software	769
Chapter 35	Configuring Secure Web Access to a Device	771
	Secure Web Access Overview	771
	Generating SSL Certificates	771
	Configuring Secure Web Access	772
	Establishing J-Web Sessions	772
Chapter 36	Configuring a Device Using J-Web	775
	Configuring Basic Settings	776
	J-Web Configuration Pages Overview	778
	Editing a Configuration	779
	J-Web Commit Options Guidelines	782
	Committing a Configuration	783
Chapter 37	Managing J-Web Sessions and Users	785
	Setting J-Web Session Limits	785
	Terminating J-Web Sessions	785
Part 8	Troubleshooting	
Chapter 38	Troubleshooting the J-Web User Interface	789
	Lost Router Connectivity	789
	Unpredictable J-Web Behavior	789
	No J-Web Access	789
Guide 4	Administration Guide for Security Devices	
Part 9	User Access and Authentication	
Chapter 39	User Access and Authentication Overview	795
	Understanding Login Classes	795
	Permission Bits	796
	Denying or Allowing Individual Commands	798
	Understanding User Accounts	798
	Understanding Junos OS Access Privilege Levels	799
	Junos OS Login Class Permission Flags	799
	Allowing or Denying Individual Commands for Junos OS Login Classes	803
	Understanding User Authentication Methods	804
	Hardening Shared Secrets in Junos OS	804
	Understanding Hardening Shared Secrets	804
	Chassis Cluster Considerations	806

Chapter 40	Configuring Junos OS User Accounts	807
	Example: Configuring New Users	807
	Understanding Template Accounts	810
	Example: Creating Template Accounts	810
	Understanding Administrative Roles	813
	Example: Configuring Administrative Roles	815
	Handling Authorization Failure	822
	Example: Configuring System Retry Options	823
Chapter 41	Configuring User Access Privileges	829
	Configuring Access Privilege Levels	829
	Example: Configuring User Permissions with Access Privilege Levels	830
	Specifying Access Privileges for Junos OS Operational Mode Commands	830
	Example: Configuring User Permissions with Access Privileges for Operational Mode Commands	833
	Specifying Access Privileges for Junos OS Configuration Mode Hierarchies	834
	Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements	835
Chapter 42	Permissions Flags for User Access Privileges	839
	Access Privilege User Permission Flags Overview	840
	access	841
	access-control	842
	admin	843
	admin-control	844
	all-control	844
	clear	845
	configure	895
	control	896
	field	896
	firewall	896
	firewall-control	897
	floppy	898
	flow-tap	898
	flow-tap-control	899
	flow-tap-operation	899
	idp-profiler-operation	899
	interface	900
	interface-control	901
	maintenance	901
	network	908
	pgcp-session-mirroring	910
	pgcp-session-mirroring-control	910
	reset	911
	rollback	912
	secret	912
	secret-control	913
	security	914
	security-control	918

	shell	921
	snmp	921
	system	921
	system-control	924
	trace	925
	trace-control	930
	view	935
	view-configuration	1008
Chapter 43	Configuring Authentication Methods	1011
	Configuring RADIUS Server Authentication	1011
	Example: Configuring a RADIUS Server for System Authentication	1014
	Configuring TACACS+ Authentication	1017
	Configuring TACACS+ Server Details	1017
	Specifying a Source Address for the Junos OS to Access External TACACS+ Servers	1018
	Configuring the Same Authentication Service for Multiple TACACS+ Servers	1018
	Configuring Juniper Networks Vendor-Specific TACACS+ Attributes	1019
	Example: Configuring a TACACS+ Server for System Authentication	1019
	Example: Configuring Authentication Order	1022
Part 10	Configuring Remote Access to an SRX Series Appliances	
Chapter 44	Configuring Secure Web Access	1027
	Secure Web Access Overview	1027
	Generating an SSL Certificate Using the openssl Command	1028
	Generating a Self-Signed SSL Certificate	1028
	Manually Generating Self-Signed SSL Certificates	1029
	Configuring Device Addresses	1029
	Enabling Access Services	1030
	Example: Configuring Secure Web Access	1031
	Adding, Editing, and Deleting Certificates on the Device	1033
Chapter 45	Setting up USB Modems for Remote Management	1035
	USB Modem Interface Overview	1035
	USB Modem Interfaces	1036
	Dialer Interface Rules	1036
	How the Device Initializes USB Modems	1037
	USB Modem Configuration Overview	1038
	Example: Configuring a USB Modem Interface	1040
	Example: Configuring a Dialer Interface	1042
	Example: Configuring a Dialer Interface for USB Modem Dial-In	1046
	Configuring a Dial-Up Modem Connection Remotely	1048
	Connecting to the Device Remotely	1049
	Modifying USB Modem Initialization Commands	1049
	Resetting USB Modems	1050

Chapter 46	Configuring Telnet and SSH Access to an SRX Series Appliance	1051
	Securing the Console Port Configuration Overview	1051
	Configuring Password Retry Limits for Telnet and SSH Access	1052
	Configuring Reverse Telnet and Reverse SSH	1053
	Example: Controlling Management Access on SRX Series Devices	1054
	Example: Configuring a Filter to Block Telnet and SSH Access	1057
	The telnet Command	1062
	The ssh Command	1063
	Configuring Outbound SSH Service	1064
	Configuring the Device Identifier for Outbound SSH Connections	1064
	Sending the Public SSH Host Key to the Outbound SSH Client	1065
	Configuring Keepalive Messages for Outbound SSH Connections	1066
	Configuring a New Outbound SSH Connection	1066
	Configuring the Outbound SSH Client to Accept NETCONF as an Available Service	1066
	Configuring Outbound SSH Clients	1067
Part 11	Configuring DNS	
Chapter 47	Configuring DNS Server Caching, DNSSEC, and DNS Proxy	1071
	DNS Overview	1071
	DNS Components	1071
	DNS Server Caching	1072
	Example: Configuring the TTL Value for DNS Server Caching	1072
	DNSSEC Overview	1073
	Example: Configuring DNSSEC	1073
	Example: Configuring Keys for DNSSEC	1074
	Example: Configuring Secure Domains and Trusted Keys for DNSSEC	1074
	DNS Proxy Overview	1076
	DNS Proxy Cache	1076
	DNS Proxy with Split DNS	1076
	Dynamic Domain Name System Client	1078
	Configuring the Device as a DNS Proxy	1080
Part 12	Configuring DHCP Access Service for IP Address Management	
Chapter 48	Understanding DHCP Services	1085
	DHCP Overview	1085
	DHCP Local Server	1085
	DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction	1085
	DHCP Local Server and Address-Assignment Pools	1086
	DHCP Client	1086
	DHCP Relay Agent	1086
	DHCP Client, DHCP Relay Agent, and DHCP Local Servers	1087
	Considerations	1087
	DHCP Server, Client, and Relay Agent Overview	1088

	DHCP Settings and Restrictions Overview	1089
	Propagation of TCP/IP Settings for DHCP	1089
	DHCP Conflict Detection and Resolution	1089
	DHCP Interface Restrictions	1090
Chapter 49	Configuring a DHCP Local Server	1091
	Understanding DHCP Server Operation	1091
	DHCP Options	1091
	Compatibility with Autoinstallation	1092
	Chassis Cluster Support	1092
	DHCP Server Configuration Overview	1092
	Minimum DHCP Local Server Configuration	1093
	Configuring Address-Assignment Pools	1094
	Configuring an Address-Assignment Pool Name and Addresses	1095
	Configuring a Named Address Range for Dynamic Address Assignment	1095
	Configuring Static Address Assignments	1096
	Enabling TCP/IP Propagation on a DHCP Local Server	1096
	Verifying and Managing DHCP Local Server Configuration	1097
Chapter 50	Configuring a DHCP Client	1099
	Understanding DHCP Client Operation	1099
	Minimum DHCP Client Configuration	1099
	Configuring DHCP Client-Specific Attributes for Address-Assignment Pools	1100
	Configuring Optional DHCP Client Attributes	1101
	Verifying and Managing DHCP Client Configuration	1101
Chapter 51	Configuring a DHCP Relay Agent	1103
	Understanding DHCP Relay Agent Operation	1103
	Minimum DHCP Relay Agent Configuration	1104
	Verifying and Managing DHCP Relay Configuration	1104
Chapter 52	Configuring a DHCPv6 Local Server	1107
	DHCPv6 Server Overview	1107
	Creating a Security Policy for DHCPv6	1108
	Example: Configuring DHCPv6 Server Options	1109
	Example: Configuring an Address-Assignment Pool	1111
	Configuring a Named Address Range for Dynamic Address Assignment	1114
	Configuring Address-Assignment Pool Linking	1114
	Configuring DHCP Client-Specific Attributes	1115
	Configuring an Address-Assignment Pool for Router Advertisement	1116
	Understanding DHCPv6 Client and Server Identification	1116
Chapter 53	Configuring a DHCPv6 Client	1119
	DHCPv6 Client Overview	1120
	Minimum DHCPv6 Client Configuration	1121
	Configuring Optional DHCPv6 Client Attributes	1122
	Configuring Nontemporary Address Assignment	1123
	Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation	1124
	Configuring Auto-Prefix Delegation	1124
	Configuring the DHCPv6 Client Rapid Commit Option	1125

	Configuring a DHCPv6 Client in Autoconfig Mode	1126
	Configuring TCP/IP Propagation on a DHCPv6 Client	1126
Part 13	Managing System Files	
Chapter 54	Performing File Management Tasks	1131
	File Management Overview	1131
	Decrypting Configuration Files	1132
	Encrypting Configuration Files	1132
	Modifying the Encryption Key	1134
	Cleaning Up Files in J-Web	1134
	Cleaning Up Files with the CLI	1135
	Deleting Files	1136
	Deleting the Backup Software Image	1137
	Downloading Files	1137
	Configuring RADIUS System Accounting	1138
	Configuring Auditing of User Events on a RADIUS Server	1138
	Specifying RADIUS Server Accounting and Auditing Events	1139
	Configuring RADIUS Server Accounting	1139
	Managing Accounting Files	1141
Part 14	Working with Junos OS Licenses	
Chapter 55	Managing Junos OS Licenses	1145
	Junos OS Feature License Keys	1145
	License Key Components	1145
	License Management Fields Summary	1146
	Software Feature Licenses for SRX Series Devices	1147
	Displaying License Keys in J-Web	1152
	Downloading License Keys	1152
	Generating a License Key	1152
	Saving License Keys	1153
	Updating License Keys	1154
	Example: Adding a New License Key	1154
	Example: Deleting a License Key	1157
Part 15	Configuration Statements and Operational Commands	
Chapter 56	Configuration Statements	1161
	[edit security certificates] Hierarchy Level	1163
	[edit security ssh-known-hosts] Hierarchy Level	1164
	Groups Configuration Statement Hierarchy	1164
	System Configuration Statement Hierarchy	1165
	address-assignment (Access)	1196
	address-pool (Access)	1199
	allow-configuration	1200
	allow-configuration-regexps	1200
	authentication-key	1201
	authentication-order	1202
	boot-server (NTP)	1203

broadcast	1204
broadcast-client	1205
ciphers	1206
connection-limit	1207
client-ia-type	1208
client-identifier (dhcp-client)	1208
client-identifier (dhcpv6-client)	1209
client-list-name (SNMP)	1209
client-type	1210
deny-configuration	1210
deny-configuration-regexps	1211
destination (Accounting)	1212
dhcp-attributes (Access IPv4 Address Pools)	1213
dhcp-attributes (Access IPv6 Address Pools)	1215
dhcp-client	1216
dhcp-local-server (System Services)	1217
dhcpv6 (System Services)	1221
dhcpv6-client	1224
disable (System Services)	1225
dlv	1225
family (Security Forwarding Options)	1226
file (System Logging)	1227
forwarding-options (Security)	1230
group (System Services DHCP)	1231
host (SSH Known Hosts)	1234
hostkey-algorithm	1235
interface (System Services DHCP)	1236
interfaces (ARP)	1237
interfaces (Security Zones)	1238
interface-traceoptions (System Services DHCP)	1239
internet-options	1241
kernel-replication (System)	1242
lease-time (dhcp-client)	1242
location	1243
lockout-period	1244
macs	1245
max-pre-authentication-packets	1246
multicast-client	1246
name-server (Access)	1247
neighbor-discovery-router-advertisement (Access)	1247
ntp	1248
outbound-ssh	1249
overrides (System Services DHCP)	1251
peer (NTP)	1252
prefix	1253
proflerd	1253
proxy	1254
radius-options	1255
radius-server	1256

rapid-commit	1257
reconfigure (System Services DHCP)	1258
req-option	1259
retransmission-attempt (dhcp-client)	1260
retransmission-attempt (dhcpv6-client)	1260
retransmission-interval (dhcp-client)	1261
root-authentication	1262
single-connection	1263
server (NTP)	1264
server-address (dhcp-client)	1265
source-address (NTP, RADIUS, System Logging, or TACACS+)	1265
ssh-known-hosts	1266
static-subscribers	1267
statistics-service	1267
subscriber-management	1268
subscriber-management-helper	1268
system master password	1269
tacplus	1270
tacplus-options	1271
tacplus-server	1272
traceoptions (Outbound SSH)	1274
traceoptions (System Services DHCP)	1276
trusted-key	1278
uac-service	1279
update-router-advertisement	1280
update-server (dhcp-client)	1280
update-server (dhcpv6-client)	1280
usb-control	1281
use-interface	1281
user-id	1282
vendor-id	1282
vpn (Forwarding Options)	1283
watchdog	1283
web-management	1284
web-management (System Services)	1285
Chapter 57	
Operational Commands	1289
clear dhcp client binding	1291
clear dhcp client statistics	1292
clear dhcp relay binding	1293
clear dhcp relay statistics	1294
clear dhcp server binding	1295
clear dhcp server statistics	1296
clear dhcpv6 client binding	1297
clear dhcpv6 client statistics	1298
clear dhcpv6 server binding (Local Server)	1299
clear dhcpv6 server statistics (Local Server)	1300
clear system login lockout	1301
file archive	1302

file checksum md5	1304
file checksum sha1	1305
file checksum sha-256	1306
file compare	1307
file copy	1310
file delete	1312
file list	1313
file rename	1314
file show	1315
request dhcp client renew	1316
request dhcpv6 client renew	1317
request system autorecovery state	1318
request system decrypt password	1320
request system download abort	1321
request system download clear	1322
request system download pause	1323
request system download resume	1324
request system download start	1325
request system firmware upgrade	1326
request system license update	1327
request system power-off fpc	1328
request system services dhcp	1329
request system snapshot (SRX Series)	1330
request system software abort in-service-upgrade (ICU)	1332
request system software add (Maintenance)	1333
request system reboot	1334
request system software rollback (SRX Series)	1335
request system zeroize	1336
restart (Reset)	1338
Restart Commands Overview	1342
show chassis routing-engine (View)	1343
show cli authorization	1345
show dhcp client binding	1346
show dhcp client statistics	1349
show dhcp relay binding	1351
show dhcp relay statistics	1353
show dhcp server binding	1355
show dhcp server statistics	1357
show dhcpv6 client binding	1359
show dhcpv6 client statistics	1361
show dhcpv6 server binding (View)	1363
show dhcpv6 server statistics (View)	1367
show firewall (View)	1370
show system autorecovery state	1372
show system download	1374
show system license (View)	1376
show system login logout	1379
show system services dhcp client	1380
show system services dhcp relay-statistics	1383

show system snapshot media	1385
show system storage partitions (View SRX Series)	1386

Guide 5 Network Management Administration Guide for Routing Devices

Part 16	Overview
Chapter 58	Network Management Overview 1393
	Understanding Device Management Functions in Junos OS 1393
	Understanding the Integrated Local Management Interface 1396
Chapter 59	Introduction to Network Monitoring 1397
	Monitoring Overview 1397
	Diagnostic Tools Overview 1398
	J-Web Diagnostic Tools 1398
	CLI Diagnostic Commands 1399
Part 17	Network Monitoring Using SNMP
Chapter 60	SNMP Overview 1403
	Understanding SNMP Implementation in Junos OS 1403
	SNMPv3 Overview 1406
Chapter 61	SNMP MIBs and Traps Supported by Junos OS 1409
	Standard SNMP MIBs Supported by Junos OS 1409
	Enterprise-Specific SNMP MIBs Supported by Junos OS 1427
	Enterprise-Specific MIBs and Supported Devices 1439
	SNMP MIB Objects Supported by Junos OS for the SNMP Set Operation . . . 1449
	Standard SNMP Traps Supported on Devices Running Junos OS 1456
	Juniper Networks Enterprise-Specific SNMP Traps 1456
Chapter 62	Loading MIB Files to a Network Management System 1459
	Loading MIB Files to a Network Management System 1459
Chapter 63	Configuring SNMP 1463
	Configuration Statements at the [edit snmp] Hierarchy Level 1464
	Optimizing the Network Management System Configuration for the Best
	Results 1467
	Changing the Polling Method from Column-by-Column to Row-by-Row . . 1467
	Reducing the Number of Variable Bindings per PDU 1468
	Increasing Timeout Values in Polling and Discovery Intervals 1468
	Reducing Incoming Packet Rate at the snmpd 1468
	Configuring Options on Managed Devices for Better SNMP Response Time . . 1469
	Enabling the stats-cache-lifetime Option 1469
	Filtering Out Duplicate SNMP Requests 1469
	Excluding Interfaces That Are Slow in Responding to SNMP Queries . . . 1470
	Configuring SNMP on Devices Running Junos OS 1471
	Configuring Basic Settings for SNMPv1 and SNMPv2 1471
	Configuring Basic Settings for SNMPv3 1471

Configuring System Name, Location, Description, and Contact Information	1473
Configuring the System Contact on a Device Running Junos OS	1474
Configuring the System Location for a Device Running Junos OS	1475
Configuring the System Description on a Device Running Junos OS	1475
Configuring SNMP Details	1476
Configuring a Different System Name	1477
Configuring the Commit Delay Timer	1478
Filtering Duplicate SNMP Requests	1478
Configuring SNMP Communities	1479
Examples: Configuring the SNMP Community String	1482
Adding a Group of Clients to an SNMP Community	1482
Configuring a Proxy SNMP Agent	1484
Configuring SNMP Traps	1485
Configuring SNMP Trap Options and Groups on a Device Running Junos OS	1487
Configuring SNMP Trap Options	1487
Configuring the Source Address for SNMP Traps	1488
Configuring the Agent Address for SNMP Traps	1490
Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps	1491
Configuring SNMP Trap Groups	1491
Example: Configuring SNMP Trap Groups	1493
Configuring the Interfaces on Which SNMP Requests Can Be Accepted	1494
Example: Configuring Secured Access List Checking	1494
Filtering Interface Information Out of SNMP Get and GetNext Output	1495
Configuring MIB Views	1496
Example: Ping Proxy MIB	1497
Chapter 64	
Configuring SNMPv3	1499
Complete SNMPv3 Configuration Statements	1500
Minimum SNMPv3 Configuration on a Device Running Junos OS	1502
Example: SNMPv3 Configuration	1503
Configuring the Local Engine ID	1506
Creating SNMPv3 Users	1507
Example: Creating SNMPv3 Users	1508
Configuring the SNMPv3 Authentication Type	1509
Configuring MD5 Authentication	1509
Configuring SHA Authentication	1509
Configuring No Authentication	1510
Configuring the SNMPv3 Encryption Type	1510
Configuring the Advanced Encryption Standard Algorithm	1510
Configuring the Data Encryption Algorithm	1511
Configuring Triple DES	1511
Configuring No Encryption	1511
Defining Access Privileges for an SNMP Group	1512
Configuring the Access Privileges Granted to a Group	1513
Configuring the Group	1513
Configuring the Security Model	1514

Configuring the Security Level	1514
Associating MIB Views with an SNMP User Group	1514
Configuring the Notify View	1515
Configuring the Read View	1515
Configuring the Write View	1516
Example: Configuring the Access Privileges Granted to a Group	1516
Assigning Security Model and Security Name to a Group	1517
Configuring the Security Model	1517
Assigning Security Names to Groups	1518
Configuring the Group	1518
Example: Security Group Configuration	1519
Configuring SNMPv3 Traps on a Device Running Junos OS	1519
Configuring the SNMPv3 Trap Notification	1520
Example: Configuring SNMPv3 Trap Notification	1521
Configuring the Trap Notification Filter	1522
Configuring the Trap Target Address	1522
Configuring the Address	1523
Configuring the Address Mask	1523
Configuring the Port	1524
Configuring the Routing Instance	1524
Configuring the Trap Target Address	1524
Applying Target Parameters	1525
Example: Configuring the Tag List	1525
Defining and Configuring the Trap Target Parameters	1526
Applying the Trap Notification Filter	1527
Configuring the Target Parameters	1527
Configuring the Message Processing Model	1527
Configuring the Security Model	1528
Configuring the Security Level	1528
Configuring the Security Name	1528
Configuring SNMP Informs	1529
Configuring the Remote Engine and Remote User	1530
Example: Configuring the Remote Engine ID and Remote User	1531
Configuring the Inform Notification Type and Target Address	1534
Example: Configuring the Inform Notification Type and Target Address	1536
Configuring the SNMPv3 Community	1536
Configuring the Community Name	1537
Configuring the Context	1538
Configuring the Security Names	1538
Configuring the Tag	1538
Example: Configuring an SNMPv3 Community	1539
Chapter 65	
Configuring SNMP for Routing Instances	1541
Understanding SNMP Support for Routing Instances	1541
SNMP MIBs Supported for Routing Instances	1542
Support Classes for MIB Objects	1552
SNMP Traps Supported for Routing Instances	1553

	Identifying a Routing Instance	1554
	Enabling SNMP Access over Routing Instances	1555
	Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community	1555
	Example: Configuring Interface Settings for a Routing Instance	1556
	Configuring Access Lists for SNMP Access over Routing Instances	1557
Chapter 66	Configuring SNMP Remote Operations	1559
	SNMP Remote Operations Overview	1559
	SNMP Remote Operation Requirements	1560
	Setting SNMP Views	1560
	Example: Setting SNMP Views	1560
	Setting Trap Notification for Remote Operations	1561
	Example: Setting Trap Notification for Remote Operations	1561
	Using Variable-Length String Indexes	1561
	Example: Set Variable-Length String Indexes	1561
	Enabling Logging	1562
	Using the Ping MIB for Remote Monitoring Devices Running Junos OS	1562
	Starting a Ping Test	1562
	Using Multiple Set Protocol Data Units (PDUs)	1563
	Using a Single Set PDU	1563
	Monitoring a Running Ping Test	1564
	pingResultsTable	1564
	pingProbeHistoryTable	1565
	Generating Traps	1566
	Gathering Ping Test Results	1567
	Stopping a Ping Test	1568
	Interpreting Ping Variables	1568
	Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS	1569
	Starting a Traceroute Test	1570
	Using Multiple Set PDUs	1570
	Using a Single Set PDU	1570
	Monitoring a Running Traceroute Test	1571
	traceRouteResultsTable	1571
	traceRouteProbeResultsTable	1572
	traceRouteHopsTable	1573
	Generating Traps	1574
	Monitoring Traceroute Test Completion	1575
	Gathering Traceroute Test Results	1576
	Stopping a Traceroute Test	1577
	Interpreting Traceroute Variables	1578
Chapter 67	Tracing SNMP Activity	1579
	Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS	1579
	Checking for MIB Objects Registered with the snmpd	1579
	Tracking SNMP Activity	1580
	Monitoring SNMP Statistics	1582
	Checking CPU Utilization	1583

	Checking Kernel and Packet Forwarding Engine Response	1584
	Tracing SNMP Activity on a Device Running Junos OS	1585
	Configuring the Number and Size of SNMP Log Files	1586
	Configuring Access to the Log File	1586
	Configuring a Regular Expression for Lines to Be Logged	1587
	Configuring the Trace Operations	1587
	Example: Tracing SNMP Activity	1588
Chapter 68	SNMP FAQs	1591
	Junos OS SNMP FAQ Overview	1591
	Junos OS SNMP FAQs	1592
	Junos OS SNMP Support FAQs	1592
	Junos OS MIBs FAQs	1593
	Junos OS SNMP Configuration FAQs	1600
	SNMPv3 FAQs	1604
	SNMP Interaction with Juniper Networks Devices FAQs	1606
	SNMP Traps and Informs FAQs	1608
	Junos OS Dual Routing Engine Configuration FAQs	1614
	SNMP Support for Routing Instances FAQs	1615
	SNMP Counters FAQs	1616
Part 18	Remote Monitoring (RMON) with SNMP	
Chapter 69	RMON Overview	1621
	Understanding RMON Alarms	1621
	alarmTable	1621
	jnxRmonAlarmTable	1622
	Understanding RMON Events	1623
	eventTable	1623
Chapter 70	Configuring RMON Alarms and Events	1625
	Understanding RMON Alarms and Events Configuration	1625
	Minimum RMON Alarm and Event Entry Configuration	1626
	Configuring an Alarm Entry and Its Attributes	1626
	Configuring the Alarm Entry	1627
	Configuring the Description	1627
	Configuring the Falling Event Index or Rising Event Index	1627
	Configuring the Falling Threshold or Rising Threshold	1627
	Configuring the Interval	1628
	Configuring the Falling Threshold Interval	1628
	Configuring the Request Type	1629
	Configuring the Sample Type	1629
	Configuring the Startup Alarm	1629
	Configuring the System Log Tag	1630
	Configuring the Variable	1630
	Configuring an Event Entry and Its Attributes	1630
	Example: Configuring an RMON Alarm and Event Entry	1631

Chapter 71	Monitoring RMON Alarms and Events	1633
	Using alarmTable to Monitor MIB Objects	1633
	Creating an Alarm Entry	1633
	Configuring the Alarm MIB Objects	1633
	alarmInterval	1634
	alarmVariable	1634
	alarmSampleType	1634
	alarmValue	1634
	alarmStartupAlarm	1634
	alarmRisingThreshold	1635
	alarmFallingThreshold	1635
	alarmOwner	1635
	alarmRisingEventIndex	1635
	alarmFallingEventIndex	1635
	Activating a New Row in alarmTable	1636
	Modifying an Active Row in alarmTable	1636
	Deactivating a Row in alarmTable	1636
	Using eventTable to Log Alarms	1636
	Creating an Event Entry	1636
	Configuring the MIB Objects	1637
	eventType	1637
	eventCommunity	1637
	eventOwner	1637
	eventDescription	1638
	Activating a New Row in eventTable	1638
	Deactivating a Row in eventTable	1638
Chapter 72	Using RMON to Monitor Network Service Quality	1639
	Understanding RMON for Monitoring Service Quality	1639
	Setting Thresholds	1639
	RMON Command-Line Interface	1640
	RMON Event Table	1641
	RMON Alarm Table	1641
	Troubleshooting RMON	1642
	Understanding Measurement Points, Key Performance Indicators, and Baseline Values	1643
	Measurement Points	1643
	Basic Key Performance Indicators	1644
	Setting Baselines	1644
	Defining and Measuring Network Availability	1644
	Defining Network Availability	1645
	Monitoring the SLA and the Required Bandwidth	1646
	Measuring Availability	1647
	Real-Time Performance Monitoring	1647
	Measuring Health	1650
	Measuring Performance	1656
	Measuring Class of Service	1659
	Inbound Firewall Filter Counters per Class	1660
	Monitoring Output Bytes per Queue	1661

	Dropped Traffic	1662
Part 19	Health Monitoring with SNMP	
Chapter 73	Configuring Health Monitoring	1667
	Configuring Health Monitoring on Devices Running Junos OS	1667
	Monitored Objects	1668
	Minimum Health Monitoring Configuration	1669
	Configuring the Falling Threshold or Rising Threshold	1669
	Configuring the Interval	1669
	Log Entries and Traps	1670
	Example: Configuring Health Monitoring	1670
Part 20	Gathering Statistics for Accounting Purposes Using Accounting Options, Source Class Usage and Destination Class Usage Options	
Chapter 74	Accounting Options, Source Class Usage and Destination Class Usage Options Overview	1673
	Accounting Options Overview	1673
	Understanding Source Class Usage and Destination Class Usage Options . . .	1674
Chapter 75	Configuring Accounting Options, Source Class Usage and Destination Class Usage Options	1677
	Configuration Statements at the [edit accounting-options] Hierarchy Level . .	1677
	Accounting Options Configuration	1678
	Accounting Options—Full Configuration	1679
	Minimum Accounting Options Configuration	1680
	Configuring Accounting-Data Log Files	1682
	Configuring the Storage Location of the File	1682
	Configuring the Maximum Size of the File	1683
	Configuring the Maximum Number of Files	1683
	Configuring the Start Time for File Transfer	1683
	Configuring the Transfer Interval of the File	1683
	Configuring Archive Sites	1684
	Configuring the Interface Profile	1685
	Configuring Fields	1685
	Configuring the File Information	1685
	Configuring the Interval	1686
	Example: Configuring the Interface Profile	1686
	Configuring the Filter Profile	1687
	Configuring the Counters	1688
	Configuring the File Information	1688
	Configuring the Interval	1689
	Example: Configuring a Filter Profile	1689
	Example: Configuring Interface-Specific Firewall Counters and Filter Profiles . .	1690
	Configuring SCU or DCU	1691
	Creating Prefix Route Filters in a Policy Statement	1692
	Applying the Policy to the Forwarding Table	1692
	Enabling Accounting on Inbound and Outbound Interfaces	1692

	Configuring SCU on a Virtual Loopback Tunnel Interface	1693
	Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC	1693
	Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface	1694
	Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface	1694
	Configuring Class Usage Profiles	1695
	Configuring a Class Usage Profile	1695
	Configuring the File Information	1695
	Configuring the Interval	1696
	Creating a Class Usage Profile to Collect Source Class Usage Statistics . .	1696
	Creating a Class Usage Profile to Collect Destination Class Usage Statistics	1696
	Configuring the MIB Profile	1697
	Configuring the File Information	1697
	Configuring the Interval	1698
	Configuring the MIB Operation	1698
	Configuring MIB Object Names	1698
	Example: Configuring a MIB Profile	1698
	Configuring the Routing Engine Profile	1699
	Configuring Fields	1699
	Configuring the File Information	1700
	Configuring the Interval	1700
	Example: Configuring a Routing Engine Profile	1700
Part 21	Configuring Monitoring Options	
Chapter 76	Configuring Interface Alarms	1703
	Alarm Overview	1703
	Alarm Types	1703
	Alarm Severity	1704
	Alarm Conditions	1704
	Interface Alarm Conditions	1705
	System Alarm Conditions	1708
	Example: Configuring Interface Alarms	1709
	Monitoring Active Alarms on a Device	1711
	Monitoring Alarms	1712
Chapter 77	Using RPM to Measure Network Performance	1715
	RPM Overview	1715
	RPM Probes	1716
	RPM Tests	1716
	Probe and Test Intervals	1716
	Jitter Measurement with Hardware Timestamping	1717
	RPM Statistics	1717
	RPM Thresholds and Traps	1718
	RPM for BGP Monitoring	1719
	IPv6 RPM Probes	1719
	Guidelines for Configuring RPM Probes for IPv6	1719

	RPM Support for VPN Routing and Forwarding	1721
	Example: Configuring Basic RPM Probes	1721
	Example: Configuring RPM Using TCP and UDP Probes	1725
	Example: Configuring RPM Probes for BGP Monitoring	1728
	Directing RPM Probes to Select BGP Devices	1730
	Configuring IPv6 RPM Probes	1731
	Tuning RPM Probes	1732
	RPM Configuration Options	1732
	Monitoring RPM Probes	1736
Chapter 78	Configuring IP Monitoring	1741
	IP Monitoring Overview	1741
	Understanding IP Monitoring Test Parameters	1742
	Example: Configuring IP Monitoring on Branch SRX Series Devices	1743
	Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups	1745
	Example: Configuring IP Monitoring on High-End SRX Series Devices	1746
	Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring	1751
Part 22	Monitoring Common Security Features	
Chapter 79	Displaying Real-Time Information from Device to Host	1757
	Displaying Real-Time Monitoring Information	1757
	Displaying Multicast Path Information	1759
Chapter 80	Monitoring Application Layer Gateways Features	1763
	Monitoring H.323 ALG Information	1763
	Monitoring MGCP ALGs	1764
	Monitoring MGCP ALG Calls	1764
	Monitoring MGCP ALG Counters	1765
	Monitoring MGCP ALG Endpoints	1766
	Monitoring SCCP ALGs	1767
	Monitoring SCCP ALG Calls	1767
	Monitoring SCCP ALG Counters	1768
	Monitoring SIP ALGs	1769
	Monitoring SIP ALG Calls	1770
	Monitoring SIP ALG Counters	1770
	Monitoring SIP ALG Rate Information	1772
	Monitoring SIP ALG Transactions	1773
	Monitoring Voice ALG H.323	1774
	Monitoring Voice ALG MGCP	1776
	Monitoring Voice ALG SCCP	1779
	Monitoring Voice ALG SIP	1782
	Monitoring Voice ALG Summary	1787
Chapter 81	Monitoring Interfaces and Switching Functions	1789
	Displaying Real-Time Interface Information	1789
	Monitoring Address Pools	1791
	Monitoring Ethernet Switching	1792

	Monitoring GVRP	1793
	Monitoring Interfaces	1794
	Monitoring MPLS Traffic Engineering Information	1795
	Monitoring MPLS Interfaces	1796
	Monitoring MPLS LSP Information	1796
	Monitoring MPLS LSP Statistics	1797
	Monitoring RSVP Session Information	1798
	Monitoring MPLS RSVP Interfaces Information	1799
	Monitoring PPP	1800
	Monitoring PPPoE	1801
	Monitoring Spanning Tree	1805
	Monitoring the WAN Acceleration Interface	1806
Chapter 82	Monitoring NAT	1807
	Monitoring NAT	1807
	Monitoring Source NAT Information	1807
	Monitoring Destination NAT Information	1813
	Monitoring Static NAT Information	1815
	Monitoring Incoming Table Information	1816
	Monitoring Interface NAT Port Information	1817
Chapter 83	Monitoring Security Policies	1819
	Monitoring Policy Statistics	1819
	Monitoring Routing Information	1820
	Monitoring Route Information	1820
	Monitoring RIP Routing Information	1822
	Monitoring OSPF Routing Information	1823
	Monitoring BGP Routing Information	1825
	Monitoring Security Events by Policy	1827
	Monitoring Security Features	1829
	Monitoring Policies	1829
	Checking Policies	1832
	Monitoring Screen Counters	1835
	Monitoring IDP Status	1837
	Monitoring Flow Gate Information	1838
	Monitoring Firewall Authentication Table	1839
	Monitoring Firewall Authentication History	1841
	Monitoring 802.1x	1843
Chapter 84	Monitoring Events, Services and System	1845
	Monitoring DHCP Client Bindings	1845
	Monitoring Events	1845
	Monitoring the System	1848
	Monitoring System Properties for SRX Series Devices	1848
	Monitoring Chassis Information	1850
	System Health Management for Branch SRX Series Devices	1852
Chapter 85	Monitoring Unified Threat Management Features	1855
	Monitoring Antivirus Scan Engine Status	1855
	Monitoring Antivirus Scan Results	1856

	Monitoring Antivirus Session Status	1858
	Monitoring Content Filtering Configurations	1858
	Monitoring Reports	1859
	Threats Monitoring Report	1859
	Traffic Monitoring Report	1864
	Monitoring Web Filtering Configurations	1866
Chapter 86	Monitoring VPNs	1867
	Monitoring VPNs	1867
	Monitoring IKE Gateway Information	1867
	Monitoring IPsec VPN—Phase I	1871
	Monitoring IPsec VPN—Phase II	1872
	Monitoring IPsec VPN Information	1873
Part 23	Resource Monitoring of Memory Regions and Types Using CLI and SNMP Queries	
Chapter 87	Effective Troubleshooting of System Performance With Resource Monitoring Methodology	1881
	Resource Monitoring Usage Computation Overview	1881
	Resource Monitoring and Usage Computation For Trio-Based Line Cards	1882
	Resource Monitoring and Usage Computation For I-Chip-Based Line Cards	1882
	Resource Monitoring Mechanism on MX Series Routers Overview	1884
	Examining the Utilization of Memory Resource Regions Using show Commands	1885
	Diagnosing and Debugging System Performance By Configuring Memory Resource Usage Monitoring on MX Series Routers	1886
	Managed Objects for Ukernl Memory for a Packet Forwarding Engine in an FPC Slot	1888
	Managed Objects for Packet Forwarding Engine Memory Statistics Data	1889
	Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot	1889
	jnxPfeMemoryErrorsTable	1890
	pfeMemoryErrors	1890
Part 24	Troubleshooting	
Chapter 88	Configuring Data Path Debugging and Trace Options	1893
	Understanding Data Path Debugging for SRX Series Devices	1893
	Debugging the Data Path (CLI Procedure)	1894
	Example: Configuring End-to-End Debugging on a High-End SRX Series Device	1895
	Understanding Security Debugging Using Trace Options	1899
	Setting Security Trace Options (CLI Procedure)	1899
	Displaying Log and Trace Files	1900
	Displaying Output for Security Trace Options	1901
	Displaying Multicast Trace Operations	1901

	Using the J-Web Traceroute Tool	1902
	J-Web Traceroute Results and Output Summary	1904
	Understanding Flow Debugging Using Trace Options	1905
	Setting Flow Debugging Trace Options (CLI Procedure)	1905
	Displaying a List of Devices	1906
Chapter 89	Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits	1909
	MPLS Connection Checking Overview	1909
	Configuring Ping MPLS	1911
	Using the ping Command	1912
	Using the J-Web Ping Host Tool	1914
	J-Web Ping Host Results and Output Summary	1916
	Using the J-Web Ping MPLS Tool	1917
	J-Web Ping MPLS Results and Output Summary	1920
	Pinging Layer 2 Circuits	1921
	Pinging Layer 2 VPNs	1922
	Pinging Layer 3 VPNs	1923
	Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs	1924
Chapter 90	Using Packet Capture to Analyze Network Traffic	1927
	Packet Capture Overview	1927
	Packet Capture on Device Interfaces	1928
	Firewall Filters for Packet Capture	1929
	Packet Capture Files	1929
	Analysis of Packet Capture Files	1929
	Example: Enabling Packet Capture on a Device	1930
	Example: Configuring Packet Capture on an Interface	1933
	Example: Configuring a Firewall Filter for Packet Capture	1935
	Example: Configuring Packet Capture for Datapath Debugging	1937
	Disabling Packet Capture	1940
	Deleting Packet Capture Files	1941
	Changing Encapsulation on Interfaces with Packet Capture Configured	1941
	Displaying Packet Headers	1943
	Using the J-Web Packet Capture Tool	1947
	J-Web Packet Capture Results and Output Summary	1950
Chapter 91	Troubleshooting Security Devices	1953
	Recovering the Root Password for SRX Series Devices	1953
	Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)	1954
	Troubleshooting the Link Services Interface	1955
	Determine Which CoS Components Are Applied to the Constituent Links	1955
	Determine What Causes Jitter and Latency on the Multilink Bundle	1957
	Determine If LFI and Load Balancing Are Working Correctly	1957
	Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device	1964
	Troubleshooting Security Policies	1964
	Checking a Security Policy Commit Failure	1964
	Verifying a Security Policy Commit	1965

	Debugging Policy Lookup	1965
	Understanding Log Error Messages for Troubleshooting ISSU-Related Problems	1966
	Chassisd Process Errors	1966
	Kernel State Synchronization	1966
	Installation Related Errors	1966
	ISSU Support Related Errors	1967
	Redundancy Group Failover Errors	1967
	Initial Validation Checks Fail	1967
Part 25	Configuration Statements and Operational Commands	
Chapter 92	Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options	1971
	accounting-options	1972
	archive-sites	1972
	class-usage-profile	1973
	counters	1974
	destination-classes	1974
	fields (for Interface Profiles)	1975
	fields (for Routing Engine Profiles)	1976
	file (Associating with a Profile)	1977
	file (Configuring a Log File)	1978
	files	1979
	filter-profile	1980
	interface-profile	1981
	interval	1982
	mib-profile	1983
	mpls (Security Forwarding Options)	1984
	nonpersistent	1985
	object-names	1985
	operation	1986
	packet-capture	1987
	packet-filter	1988
	redundancy-group (Chassis Cluster)	1989
	retry-interval (Chassis Cluster)	1990
	routing-engine-profile	1991
	size	1992
	source-classes	1992
	start-time	1993
	traceoptions (System Accounting)	1994
	transfer-interval	1995
Chapter 93	Configuration Statements: Chassis Cluster	1997
	cluster (Chassis)	1998
	global-threshold	1999
	global-weight	2000
	ip-monitoring	2001
	ip-monitoring (Services)	2002
	next-hop	2003

Chapter 94	Configuration Statements: Datapath Debug	2005
	action-profile	2006
	capture-file (Security)	2007
	datapath-debug	2008
	flow (Security Flow)	2010
	icmp	2012
	maximum-capture-size (Datapath Debug)	2012
	traceoptions (Security Datapath Debug)	2013
Chapter 95	Configuration Statements: Health Monitoring	2015
	falling-threshold	2015
	health-monitor	2016
	interval	2016
	rising-threshold	2017
Chapter 96	Configuration Statements: Remote Monitoring (RMON)	2019
	alarm (SNMP RMON)	2020
	community	2021
	description	2021
	event	2022
	falling-event-index	2022
	falling-threshold	2023
	falling-threshold-interval	2024
	interval	2024
	request-type	2025
	rising-event-index	2026
	rising-threshold	2026
	rmon	2027
	sample-type	2027
	startup-alarm	2028
	syslog-subtag	2028
	type	2029
	variable	2029
Chapter 97	Configuration Statements: Resource Monitoring for Memory Regions . .	2031
	[edit system services resource-monitor] Hierarchy Level	2031
	free-fw-memory-watermark (Resource Monitor)	2032
	free-heap-memory-watermark (Resource Monitor)	2033
	free-nh-memory-watermark (Resource Monitor)	2033
	high-threshold (Resource Monitor)	2034
	no-logging (Resource Monitor)	2034
	resource-monitor	2035
	resource-type contiguous-pages (Resource Monitor)	2036
	resource-type free-dwords (Resource Monitor)	2037
	resource-type free-pages (Resource Monitor)	2038
	services (Resource Monitor)	2039
	traceoptions (Resource Monitor)	2040

Chapter 98	Configuration Statements: Security Alarms	2041
	decryption-failures	2041
	idp (Security Alarms)	2042
Chapter 99	Configuration Statements: SNMP	2043
	access-list	2044
	agent-address	2045
	alarm-id	2046
	alarm-list-name	2047
	alarm-management	2048
	alarm-state	2049
	authorization	2050
	categories	2050
	client-list	2051
	client-list-name	2051
	clients	2052
	commit-delay	2052
	community (SNMP)	2053
	contact (SNMP)	2054
	description	2054
	destination-port	2055
	enterprise-oid	2055
	filter-duplicates	2056
	filter-interfaces	2056
	interface (SNMP)	2057
	location (SNMP)	2057
	logical-system	2058
	logical-system-trap-filter	2059
	name	2059
	nonvolatile	2060
	oid	2060
	proxy (snmp)	2061
	routing-instance	2062
	routing-instance-access	2063
	snmp	2063
	source-address	2064
	targets	2064
	traceoptions (SNMP)	2065
	trap-group	2067
	trap-options	2068
	version (SNMP)	2069
	view (Associating a MIB View with a Community)	2069
	view (Configuring a MIB View)	2070
Chapter 100	Configuration Statements: SNMPv3	2071
	address	2072
	address-mask	2073
	authentication-md5	2073
	authentication-none	2074

authentication-password	2075
authentication-sha	2076
community-name	2077
context (SNMPv3)	2078
engine-id	2079
group (Configuring Group Name)	2080
group (Defining Access Privileges for an SNMPv3 Group)	2081
retry-count	2081
timeout	2082
local-engine	2083
message-processing-model	2084
notify	2085
notify-filter (Applying to the Management Target)	2086
notify-filter (Configuring the Profile Name)	2086
notify-view	2087
oid	2087
parameters	2088
port	2088
privacy-3des	2089
privacy-aes128	2090
privacy-des	2091
privacy-none	2091
privacy-password	2092
read-view	2093
remote-engine	2094
routing-instance	2095
security-level (Defining Access Privileges)	2096
security-level (Generating SNMP Notifications)	2097
security-model (Access Privileges)	2098
security-model (Group)	2099
security-model (SNMP Notifications)	2099
security-name (Community String)	2100
security-name (Security Group)	2101
security-name (SNMP Notifications)	2102
security-to-group	2103
snmp-community	2103
tag	2104
tag-list	2104
target-address	2105
target-parameters	2106
type	2107
user	2107
usm	2108
v3	2110
vacm	2112
write-view	2113

Chapter 101	Operational Commands	2115
	clear chassis cluster ip-monitoring failure-count	2117
	clear chassis cluster ip-monitoring failure-count ip-address	2118
	clear ilmi statistics	2119
	clear snmp history	2120
	clear snmp statistics	2121
	request pppoe connect	2123
	request pppoe disconnect	2124
	request services ip-monitoring preempt-restore policy	2125
	request snmp spoof-trap	2126
	show chassis alarms	2132
	show chassis cluster ip-monitoring status redundancy-group	2134
	show interfaces (SRX Series)	2137
	show interfaces snmp-index	2168
	show interfaces summary	2169
	show ilmi statistics	2171
	show security alarms	2174
	show security datapath-debug capture	2178
	show security datapath-debug counter	2179
	show security monitoring	2180
	show security monitoring fpc fpc-number	2182
	show security monitoring performance session	2185
	show security monitoring performance spu	2186
	show services ip-monitoring status	2187
	show snmp health-monitor	2191
	show snmp inform-statistics	2198
	show snmp mib	2200
	show snmp rmon	2203
	show snmp statistics	2207
	show snmp stats-response-statistics	2215
	show snmp v3	2217
	show system alarms	2220
	show system resource-monitor fpc	2221

Guide 6 Standards Reference

Part 26	Overview	
Chapter 102	Accessing Standards Documents	2227
	Accessing Standards Documents on the Internet	2227
Part 27	Supported Standards	
Chapter 103	Chassis and System Standards	2231
	Supported BFD Standards	2231
	Supported BOOTP and DHCP Standards	2232
	Supported Mobile IP Standards	2233
	Supported Network Management Standards	2233
	Supported RADIUS and TACACS+ Standards for User Authentication	2244

	Supported System Access Standards	2244
	Supported Time Synchronization Standard	2245
Chapter 104	Interface Standards	2247
	Supported ATM Interface Standards	2247
	Supported Ethernet Interface Standards	2248
	Supported Frame Relay Interface Standards	2249
	Supported GRE and IP-IP Interface Standards	2249
	Supported PPP Interface Standards	2250
	Supported SDH and SONET Interface Standards	2251
	Supported Serial Interface Standards	2252
	Supported T3 Interface Standard	2252
Chapter 105	Layer 2 Standards	2253
	Supported Layer 2 Networking Standards	2253
	Supported L2TP Standards	2254
	Supported VPWS Standards	2254
	Supported Layer 2 VPN Standards	2255
	Supported Security Standards	2256
Chapter 106	MPLS Applications Standards	2257
	Supported GMPLS Standards	2257
	Supported LDP Standards	2258
	Supported MPLS Standards	2259
	Supported RSVP Standards	2262
Chapter 107	Open Standards	2265
	Supported Open Standards	2265
Chapter 108	Packet Processing Standards	2269
	Supported CoS Standards	2269
	Supported Packet Filtering Standards	2270
	Supported Policing Standard	2270
Chapter 109	Routing Protocol Standards	2273
	Supported Standards for BGP	2273
	Supported ES-IS Standards	2275
	Supported ICMP Router Discovery and IPv6 Neighbor Discovery Standards	2276
	Supported IP Multicast Protocol Standards	2276
	Supported IPv4, TCP, and UDP Standards	2278
	Supported IPv6 Standards	2280
	Supported Standards for IS-IS	2283
	Supported OSPF and OSPFv3 Standards	2284
	Supported RIP and RIPvng Standards	2286
Chapter 110	Services PIC and DPC Standards	2287
	Supported DTCP Standard	2287
	Supported Flow Monitoring and Discard Accounting Standards	2287
	Supported IPsec and IKE Standards	2288
	Supported L2TP Standards	2290
	Supported Link Services Standards	2290
	Supported NAT and SIP Standards	2291

	Supported RPM Standard	2291
	Supported Voice Services Standards	2292
Chapter 111	VPLS and VPN Standards	2293
	Supported Carrier-of-Carriers and Interprovider VPN Standards	2293
	Supported EVPN Standards	2294
	Supported Layer 2 VPN Standards	2294
	Supported Layer 3 VPN Standards	2295
	Supported Multicast VPN Standards	2296
	Supported VPLS Standards	2296
 Part 28	 Index	
	Index	2301

List of Figures

Part 1	Junos Software and Hardware Overview	
Chapter 1	Software Overview	3
	Figure 1: Configuration Selection Sequence	15
Chapter 2	Hardware Overview	27
	Figure 2: Routing Engines	29
	Figure 3: SRX345 Device Front Panel	31
	Figure 4: SRX1500 Device Front Panel	31
	Figure 5: SRX5800 Device Routing Engine	31
Part 2	Installing Junos Software	
Chapter 4	Performing a Standard or Change Category Installation	47
	Figure 6: Connecting to the Console Port on a Junos OS Device	54
Chapter 8	Upgrading Software	115
	Figure 7: Upgrading to the 64-bit Junos OS with Dual Routing Engines	120
	Figure 8: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master in Either Slot)	121
	Figure 9: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master Must Be in Slot 0)	122
Chapter 19	Overview	421
	Figure 10: Monitoring and Configuring Routers	422
	Figure 11: Committing a Configuration	424
	Figure 12: Configuration Statement Hierarchy Example	425
Chapter 22	Using Configuration Statements to Configure a Device	455
	Figure 13: Configuration Mode Hierarchy of Statements	460
Chapter 23	Committing a Junos OS Configuration	507
	Figure 14: Confirm a Configuration	513
Chapter 24	Managing Configurations	525
	Figure 15: Overriding the Current Configuration	547
	Figure 16: Using the replace Option	547
	Figure 17: Using the merge Option	547
	Figure 18: Using a Patch File	548
	Figure 19: Using the set Option	548
Chapter 25	Using Operational Commands to Monitor a Device	563
	Figure 20: Commands That Combine Other Commands	567
	Figure 21: Command Output Options	568

	Figure 22: Restarting a Process	582
Chapter 27	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	599
	Figure 23: Replacement by Object	608
Part 6	Overview	
Chapter 33	Understanding the J-Web User Interface	761
	Figure 24: J-Web Layout	763
	Figure 25: Top Pane Elements	763
	Figure 26: Main Pane Elements	764
	Figure 27: Side Pane Elements	765
Part 7	Configuring and Managing a Device Using J-Web	
Chapter 36	Configuring a Device Using J-Web	775
	Figure 28: J-Web Set Up Initial Configuration Page	777
	Figure 29: Edit Configuration Page	780
Part 9	User Access and Authentication	
Chapter 39	User Access and Authentication Overview	795
	Figure 30: Master Password Encryption	805
Part 11	Configuring DNS	
Chapter 47	Configuring DNS Server Caching, DNSSEC, and DNS Proxy	1071
	Figure 31: DNS Proxy with Split DNS	1077
	Figure 32: Dynamic DNS	1079
Part 17	Network Monitoring Using SNMP	
Chapter 64	Configuring SNMPv3	1499
	Figure 33: Inform Request and Response	1530
Chapter 65	Configuring SNMP for Routing Instances	1541
	Figure 34: SNMP Data for Routing Instances	1542
Part 18	Remote Monitoring (RMON) with SNMP	
Chapter 72	Using RMON to Monitor Network Service Quality	1639
	Figure 35: Setting Thresholds	1640
	Figure 36: Network Entry Points	1643
	Figure 37: Regional Points of Presence	1645
	Figure 38: Measurements to Each Router	1645
	Figure 39: Network Behavior During Congestion	1660
Part 21	Configuring Monitoring Options	
Chapter 77	Using RPM to Measure Network Performance	1715
	Figure 40: Sample RPM Graphs	1737

Chapter 78	Configuring IP Monitoring	1741
	Figure 41: IP Monitoring on a High-End SRX Series Device Topology Example . .	1747
Part 24	Troubleshooting	
Chapter 91	Troubleshooting Security Devices	1953
	Figure 42: PPP and MLPPP Headers	1960

List of Tables

	About the Documentation	lxi
	Table 1: Notice Icons	lxiii
	Table 2: Text and Syntax Conventions	lxiii
Part 1	Junos Software and Hardware Overview	
Chapter 1	Software Overview	3
	Table 3: Junos OS Processes	18
	Table 4: Upgraded FreeBSD Kernel Support by Hardware Platform	19
	Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD	20
	Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD	21
Chapter 2	Hardware Overview	27
	Table 7: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)	32
	Table 8: Storage Media Names	34
Part 2	Installing Junos Software	
Chapter 4	Performing a Standard or Change Category Installation	47
	Table 9: show system download Output Fields	53
	Table 10: Install Remote Summary	65
	Table 11: Upload Package Summary	66
	Table 12: Environment Variables Settings	71
Chapter 6	Configuring Automatic Installation of Configuration Files	81
	Table 13: Interfaces and Protocols for IP Address Acquisition During Autoinstallation	82
Chapter 7	Configuring Dual-Root Partitions for High Availability	95
	Table 14: Resilient Dual-Root Partition Scheme	96
	Table 15: Earlier Partition Scheme	98
	Table 16: Combinations of Junos OS Versions and Loader Software Versions	100
	Table 17: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled	102
	Table 18: Actions If Corrupt Files Are Found	103
	Table 19: Storage Media on SRX Series Devices	106
Chapter 8	Upgrading Software	115
	Table 20: Platform and Release Support for NSSU	128

	Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD	139
	Table 22: Secondary Storage Devices for SRX Series Devices	148
	Table 23: Install Package Summary	153
	Table 24: CLI Commands for Manual BIOS Upgrade	154
Chapter 10	Performing a Recovery Installation	165
	Table 25: Autorecovery Alarms	171
Chapter 11	Reinstalling Software	187
	Table 26: Checklist for Reinstalling Junos OS	187
Part 3	Installing and Managing Software Licenses	
Chapter 14	Software License Overview	223
	Table 27: Upgrade Licenses for Enhancing Port Capacity	227
	Table 28: Port Activation License Model for MX104 Routers	228
	Table 29: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers	229
	Table 30: Junos OS Feature License Model Number for M Series Routers	232
	Table 31: Junos OS Feature License Model Number for MX Series Routers	233
	Table 32: Junos OS Feature Licenses	236
	Table 33: Junos OS Feature License Model Number for SRX Series Devices	238
	Table 34: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices	242
	Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices	244
	Table 36: Junos OS EFL Part Number on EX2200 Switches	247
	Table 37: Junos OS EFL Part Number on EX2300 Switches	248
	Table 38: Junos OS EFL Part Number on EX3300 Switches	249
	Table 39: Junos OS AFL Part Number on EX3300 Switches	249
	Table 40: Junos OS EFL Part Number on EX3400 Switches	250
	Table 41: Junos OS EFL Part Number on EX4300 Switches	251
	Table 42: Junos OS AFL Part Number on EX4300 Switches	251
	Table 43: Junos OS AFL Part Number on EX4600 Switches	252
	Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches	253
Part 5	Configuration Statements and Operational Commands	
Chapter 18	Operational Commands	289
	Table 45: request system storage cleanup Output Fields	366
	Table 46: request system storage cleanup Output Fields	374
	Table 47: show system autoinstallation status Output Fields	383
	Table 48: show system autorecovery state Output Fields	385
	Table 49: show system auto-snapshot status Output Fields	394
	Table 50: show system download Output Fields	396
	Table 51: show system license Output Fields	399
	Table 52: show system license Output Fields	406
	Table 53: show system login lockout	409
	Table 54: show system snapshot Output Fields	411

	Table 55: show system storage partitions Output Fields	415
Chapter 19	Overview	421
	Table 56: CLI Configuration Mode Navigation Commands	425
Chapter 22	Using Configuration Statements to Configure a Device	455
	Table 57: Summary of Configuration Mode Commands	457
	Table 58: Configuration Mode Top-Level Statements	459
	Table 59: Forms of the configure Command	466
Chapter 24	Managing Configurations	525
	Table 60: CLI Configuration Input Types	543
Chapter 25	Using Operational Commands to Monitor a Device	563
	Table 61: Commonly Used Operational Mode Commands	565
	Table 62: Directories on the Router	574
	Table 63: show system process extensive Command Output Fields	581
Chapter 26	Filtering Command Output	587
	Table 64: Common Regular Expression Operators in Operational Mode Commands	588
Chapter 27	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	599
	Table 65: CLI Keyboard Sequences	600
	Table 66: Wildcard Characters for Specifying Interface Names	601
	Table 67: Common Regular Expressions to Use with the replace Command	602
	Table 68: Replacement Examples	603
Chapter 31	Junos OS CLI Environment Commands	709
	Table 69: show cli Output Fields	720
Part 7	Configuring and Managing a Device Using J-Web	
Chapter 35	Configuring Secure Web Access to a Device	771
	Table 70: Concurrent Web Sessions on SRX Series Devices	773
Chapter 36	Configuring a Device Using J-Web	775
	Table 71: Initial Configuration Set Up Summary	777
	Table 72: J-Web Configuration Pages Summary	779
	Table 73: J-Web Edit Configuration Links	781
	Table 74: J-Web Edit Configuration Icons	781
Part 9	User Access and Authentication	
Chapter 39	User Access and Authentication Overview	795
	Table 75: Predefined Login Classes	795
	Table 76: Permission Bits for Login Classes	796
	Table 77: Login Class Permission Flags	800
	Table 78: \$8\$-encrypted Password Format	805
Part 10	Configuring Remote Access to an SRX Series Appliances	
Chapter 45	Setting up USB Modems for Remote Management	1035

	Table 79: Default Modem Initialization Commands	1037
	Table 80: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity	1039
	Table 81: Incoming Map Options	1039
Chapter 46	Configuring Telnet and SSH Access to an SRX Series Appliance	1051
	Table 82: CLI telnet Command Options	1062
	Table 83: CLI ssh Command Options	1063
Part 12	Configuring DHCP Access Service for IP Address Management	
Chapter 49	Configuring a DHCP Local Server	1091
	Table 84: Sample DHCP Server Configuration Settings	1092
Chapter 52	Configuring a DHCPv6 Local Server	1107
	Table 85: DHCPv6 Attributes	1115
Part 13	Managing System Files	
Chapter 54	Performing File Management Tasks	1131
	Table 86: request system set-encryption-key Commands	1132
Part 14	Working with Junos OS Licenses	
Chapter 55	Managing Junos OS Licenses	1145
	Table 87: Summary of License Management Fields	1146
	Table 88: Junos OS Feature Licenses	1147
	Table 89: Junos OS Feature License Model Number for SRX Series Devices	1148
Part 15	Configuration Statements and Operational Commands	
Chapter 57	Operational Commands	1289
	Table 90: show chassis routing-engine Output Fields	1343
	Table 91: show dhcp client binding Output Fields	1346
	Table 92: show dhcp client statistics	1349
	Table 93: show dhcp relay binding Output Fields	1351
	Table 94: show dhcp relay statistics	1353
	Table 95: show dhcp server binding Output Fields	1355
	Table 96: show dhcp server statistics	1357
	Table 97: show dhcpv6 client binding Output Fields	1359
	Table 98: show dhcpv6 client statistics Output Fields	1361
	Table 99: show dhcv6p server binding Output Fields	1363
	Table 100: show dhcpv6 server statistics Output Fields	1368
	Table 101: show firewall Output Fields	1370
	Table 102: show system autorecovery state Output Fields	1372
	Table 103: show system download Output Fields	1374
	Table 104: show system license Output Fields	1376
	Table 105: show system login lockout	1379
	Table 106: show system services dhcp client Output Fields	1380
	Table 107: show system services dhcp relay-statistics Output Fields	1383

Part 16	Overview	
Chapter 58	Network Management Overview	1393
	Table 108: Device Management Features in Junos OS	1394
Chapter 59	Introduction to Network Monitoring	1397
	Table 109: J-Web Interface Troubleshoot Options	1398
	Table 110: CLI Diagnostic Command Summary	1399
Part 17	Network Monitoring Using SNMP	
Chapter 61	SNMP MIBs and Traps Supported by Junos OS	1409
	Table 111: Standard MIBs Supported on Devices Running Junos OS	1410
	Table 112: Enterprise-Specific MIBs and Supported Devices	1440
Chapter 64	Configuring SNMPv3	1499
	Table 113: Values to Use in Example	1532
Chapter 65	Configuring SNMP for Routing Instances	1541
	Table 114: MIB Support for Routing Instances (Juniper Networks MIBs)	1542
	Table 115: Class 1 MIB Objects (Standard and Juniper MIBs)	1546
	Table 116: Class 2 MIB Objects (Standard and Juniper MIBs)	1550
	Table 117: Class 3 MIB Objects (Standard and Juniper MIBs)	1551
	Table 118: Class 4 MIB Objects (Standard and Juniper MIBs)	1552
Chapter 66	Configuring SNMP Remote Operations	1559
	Table 119: Results in pingProbeHistoryTable: After the First Ping Test	1567
	Table 120: Results in pingProbeHistoryTable: After the First Probe of the Second Test	1567
	Table 121: Results in pingProbeHistoryTable: After the Second Ping Test	1568
	Table 122: traceRouteProbeHistoryTable	1576
Chapter 67	Tracing SNMP Activity	1579
	Table 123: SNMP Tracing Flags	1587
Chapter 68	SNMP FAQs	1591
	Table 124: Monitored Object Instances	1599
Part 18	Remote Monitoring (RMON) with SNMP	
Chapter 72	Using RMON to Monitor Network Service Quality	1639
	Table 125: RMON Event Table	1641
	Table 126: RMON Alarm Table	1641
	Table 127: jnxRmon Alarm Extensions	1642
	Table 128: Real-Time Performance Monitoring Configuration Options	1648
	Table 129: Health Metrics	1650
	Table 130: Counter Values for vlan-ccc Encapsulation	1656
	Table 131: Performance Metrics	1657
	Table 132: Inbound Traffic Per Class	1660
	Table 133: Inbound Counters	1661
	Table 134: Outbound Counters for ATM Interfaces	1661
	Table 135: Outbound Counters for Non-ATM Interfaces	1662

	Table 136: Dropped Traffic Counters	1662
Part 19	Health Monitoring with SNMP	
Chapter 73	Configuring Health Monitoring	1667
	Table 137: Monitored Object Instances	1668
Part 20	Gathering Statistics for Accounting Purposes Using Accounting Options, Source Class Usage and Destination Class Usage Options	
Chapter 74	Accounting Options, Source Class Usage and Destination Class Usage Options Overview	1673
	Table 138: Types of Accounting Profiles	1673
Part 21	Configuring Monitoring Options	
Chapter 76	Configuring Interface Alarms	1703
	Table 139: Interface Alarm Conditions	1705
	Table 140: System Alarm Conditions and Corrective Actions	1708
	Table 141: Alarms Monitoring Page	1713
Chapter 77	Using RPM to Measure Network Performance	1715
	Table 142: RPM Statistics	1717
	Table 143: RPM Configuration Summary	1733
	Table 144: Summary of Key RPM Output Fields	1737
Chapter 78	Configuring IP Monitoring	1741
	Table 145: Test Parameters and Default Values	1742
	Table 146: Threshold Supported and Description	1743
Part 22	Monitoring Common Security Features	
Chapter 79	Displaying Real-Time Information from Device to Host	1757
	Table 147: CLI traceroute monitor Command Options	1757
	Table 148: CLI traceroute monitor Command Output Summary	1758
	Table 149: CLI mtrace from-source Command Options	1759
	Table 150: CLI mtrace from-source Command Output Summary	1761
Chapter 80	Monitoring Application Layer Gateways Features	1763
	Table 151: Summary of Key H.323 Counters Output Fields	1763
	Table 152: Summary of Key MGCP Calls Output Fields	1765
	Table 153: Summary of Key MGCP Counters Output Fields	1765
	Table 154: Summary of Key MGCP Endpoints Output Fields	1767
	Table 155: Summary of Key SCCP Calls Output Fields	1768
	Table 156: Summary of Key SCCP Counters Output Fields	1768
	Table 157: Summary of Key SIP Calls Output Fields	1770
	Table 158: Summary of Key SIP Counters Output Fields	1770
	Table 159: Summary of Key SIP Rate Output Fields	1772
	Table 160: Summary of Key SIP Transactions Output Fields	1773
	Table 161: ALG H.323 Monitoring Page	1774

	Table 162: Voice ALG MGCP Monitoring Page	1776
	Table 163: Voice ALG SCCP Monitoring Page	1779
	Table 164: Voice ALG SIP Monitoring Page	1782
	Table 165: Voice ALG Summary Monitoring Page	1787
Chapter 81	Monitoring Interfaces and Switching Functions	1789
	Table 166: CLI monitor interface Output Control Keys	1789
	Table 167: CLI monitor interface traffic Output Control Keys	1790
	Table 168: Address Pools Monitoring Page	1791
	Table 169: Summary of Ethernet Switching Output Fields	1792
	Table 170: GVRP Monitoring Page	1793
	Table 171: Summary of Key MPLS Interface Information Output Fields	1796
	Table 172: Summary of Key MPLS LSP Information Output Fields	1796
	Table 173: Summary of Key MPLS LSP Statistics Output Fields	1798
	Table 174: Summary of Key RSVP Session Information Output Fields	1798
	Table 175: Summary of Key RSVP Interfaces Information Output Fields	1800
	Table 176: Summary of Key PPPoE Output Fields	1801
	Table 177: Spanning Tree Monitoring Page	1805
Chapter 82	Monitoring NAT	1807
	Table 178: Source NAT Monitoring Page	1807
	Table 179: Summary of Key Destination NAT Output Fields	1813
	Table 180: Summary of Key Static NAT Output Fields	1815
	Table 181: Summary of Key Incoming Table Output Fields	1816
	Table 182: Summary of Key Interface NAT Output Fields	1817
Chapter 83	Monitoring Security Policies	1819
	Table 183: Filtering Route Messages	1821
	Table 184: Summary of Key Routing Information Output Fields	1821
	Table 185: Summary of Key RIP Routing Output Fields	1822
	Table 186: Summary of Key OSPF Routing Output Fields	1824
	Table 187: Summary of Key BGP Routing Output Fields	1825
	Table 188: View Policy Log Fields	1827
	Table 189: Policy Events Detail Fields	1829
	Table 190: Security Policies Monitoring Output Fields	1830
	Table 191: Check Policies Output	1833
	Table 192: Summary of Key Screen Counters Output Fields	1835
	Table 193: Summary of IDP Status Output Fields	1838
	Table 194: Summary of Key Flow Gate Output Fields	1839
	Table 195: Summary of Key Firewall Authentication Table Output Fields	1840
	Table 196: Summary of Key Firewall Authentication History Output Fields	1841
	Table 197: Summary of Dot1X Output Fields	1843
Chapter 84	Monitoring Events, Services and System	1845
	Table 198: Summary of Key DHCP Client Binding Output Fields	1845
	Table 199: Events Monitoring Page	1846
Chapter 85	Monitoring Unified Threat Management Features	1855
	Table 200: Statistics Tab Output in the Threats Report	1860
	Table 201: Activities Tab Output in the Threats Report	1862
	Table 202: Traffic Report Output	1864

Chapter 86	Monitoring VPNs	1867
	Table 203: Summary of Key IKE SA Information Output Fields	1867
	Table 204: IPsec VPN—Phase I Monitoring Page	1871
	Table 205: IPsec VPN—Phase II Monitoring Page	1872
	Table 206: Summary of Key IPsec VPN Information Output Fields	1873
Part 23	Resource Monitoring of Memory Regions and Types Using CLI and SNMP Queries	
Chapter 87	Effective Troubleshooting of System Performance With Resource Monitoring Methodology	1881
	Table 207: jnxPfeMemoryUKernTable	1888
	Table 208: jnxPfeMemory Table	1889
	Table 209: jnxPfeMemoryForwardingTable	1889
	Table 210: jnxPfeMemoryErrorsTable	1890
	Table 211: pfeMemoryErrors	1890
Part 24	Troubleshooting	
Chapter 88	Configuring Data Path Debugging and Trace Options	1893
	Table 212: CLI mtrace monitor Command Output Summary	1902
	Table 213: Traceroute Field Summary	1903
	Table 214: J-Web Traceroute Results and Output Summary	1904
	Table 215: CLI traceroute Command Options	1906
Chapter 89	Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits	1909
	Table 216: Options for Checking MPLS Connections	1910
	Table 217: CLI ping Command Options	1912
	Table 218: J-Web Ping Host Field Summary	1914
	Table 219: Ping Host Results and Output	1916
	Table 220: J-Web Ping MPLS Field Summary	1917
	Table 221: J-Web Ping MPLS Results and Output Summary	1920
	Table 222: CLI ping mpls l2circuit Command Options	1921
	Table 223: CLI ping mpls l2vpn Command Options	1922
	Table 224: CLI ping mpls l3vpn Command Options	1923
	Table 225: CLI ping mpls ldp and ping mpls lsp-end-point Command Options	1924
Chapter 90	Using Packet Capture to Analyze Network Traffic	1927
	Table 226: CLI monitor traffic Command Options	1943
	Table 227: CLI monitor traffic Match Conditions	1945
	Table 228: CLI monitor traffic Logical Operators	1946
	Table 229: CLI monitor traffic Arithmetic, Binary, and Relational Operators	1946
	Table 230: Packet Capture Field Summary	1948
	Table 231: J-Web Packet Capture Results and Output Summary	1950
Chapter 91	Troubleshooting Security Devices	1953
	Table 232: CoS Components Applied on Multilink Bundles and Constituent Links	1956
	Table 233: PPP and MLPPP Encapsulation Overhead	1960

Part 25
Chapter 101

Table 234: Number of Packets Transmitted on a Queue	1963
---	------

Configuration Statements and Operational Commands

Operational Commands	2115
Table 235: show chassis alarms Output Fields	2132
Table 236: show chassis cluster ip-monitoring status Output Fields	2134
Table 237: show chassis cluster ip-monitoring status redundancy group Reason Fields	2135
Table 238: show interfaces Output Fields	2140
Table 239: show interfaces summary Output Fields	2169
Table 240: show ilmi statistics Output Fields	2172
Table 241: show security alarms	2175
Table 242: show security monitoring fpc fpc-number Output Fields	2182
Table 243: show services ip-monitoring status Output Fields	2187
Table 244: show snmp health-monitor Output Fields	2191
Table 245: show snmp inform-statistics Output Fields	2198
Table 246: show snmp mib Output Fields	2201
Table 247: show snmp rmon Output Fields	2203
Table 248: show snmp statistics Output Fields	2208
Table 249: show snmp statistics subagents Output Fields	2211
Table 250: show snmp stats-response-statistics Output Fields	2215
Table 251: show snmp v3 Output Fields	2218
Table 252: show system resource-monitor fpc Output Fields	2221

About the Documentation

- Documentation and Release Notes on page lxi
- Using the Examples in This Manual on page lxi
- Documentation Conventions on page lxiii
- Documentation Feedback on page lxv
- Requesting Technical Support on page lxv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:







```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

Documentation Conventions

[Table 1](#) defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

[Table 2](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

Installation and Upgrade Guide

PART 1

Junos Software and Hardware Overview

- [Software Overview on page 3](#)
- [Hardware Overview on page 27](#)

CHAPTER 1

Software Overview

- [Junos OS Overview on page 3](#)
- [Junos OS Editions on page 5](#)
- [FIPS 140-2 Security Compliance on page 5](#)
- [Junos OS Installation Packages on page 6](#)
- [Junos OS Package Names for EX Series Switches on page 7](#)
- [Software Naming Convention on page 9](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Software Package Information Security on page 11](#)
- [Junos OS Release Numbers on page 11](#)
- [Installation Media on page 12](#)
- [Installation Bundles on page 13](#)
- [Installation Modules on page 14](#)
- [Configuration Files on page 15](#)
- [Understanding Software Infrastructure and Processes on page 17](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)
- [Understanding Junos OS with Upgraded FreeBSD Snapshots on page 23](#)
- [Understanding Junos OS with Upgraded FreeBSD Disk Volumes on page 24](#)

Junos OS Overview

Juniper Networks provides high-performance network devices that create a responsive and trusted environment for accelerating the deployment of services and applications over a single network. The Junos[®] operating system (Junos OS) is the foundation of these high-performance networks.

Starting with Junos OS Release 15.1, certain hardware platforms run Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Basing Junos OS on the newer kernel (referred to as Junos OS with upgraded FreeBSD) provides Junos OS with sophisticated processing, efficiency, and security features which do not have to be reproduced in Junos OS.

Unlike other complex, monolithic software architectures, Junos OS incorporates key design and developmental differences to deliver increased network availability, operational efficiency, and flexibility. The key advantages to this approach are:

- [One Operating System on page 4](#)
- [One Modular Software Architecture on page 4](#)

One Operating System

Unlike other network operating systems that share a common name but splinter into many different programs, Junos OS is a single, cohesive operating system that is shared across all network devices and product lines. This allows Juniper Networks engineers to develop software features once and share these features across all product lines simultaneously. Because features are common to a single source, they generally are implemented the same way for all product lines, thus reducing the training required to learn different tools and methods for each product. Because all Juniper Networks products use the same code base, interoperability between products is not an issue.

One Modular Software Architecture

Although individual modules of Junos OS communicate through well-defined interfaces, each module runs in its own protected memory space, preventing one module from disrupting another. This separation enables the independent restart of each module as necessary. This is in contrast to monolithic operating systems where a malfunction in one module can ripple to other modules and cause a full system crash or restart. This modular architecture then provides for high performance, high availability, security, and device scalability not found in other operating systems.

The Junos OS is preinstalled on your Juniper Networks device when you receive it from the factory. Thus, when you first power on the device, all software starts automatically. You simply need to configure the software so that the device can participate in the network.

You can upgrade the device software as new features are added or software problems are fixed. You normally obtain new software by downloading the software installation packages from the Juniper Networks Support Web page onto your device or onto another system on your local network. You then install the software upgrade onto the device.

Juniper Networks routing platforms run only binaries supplied by Juniper Networks, and currently do not support third-party binaries. Each Junos OS image includes a digitally signed manifest of executables that are registered with the system only if the signature can be validated. Junos OS will not execute any binary without a registered signature. This feature protects the system against unauthorized software and activity that might compromise the integrity of your device.

Related Documentation

- [Junos OS Editions on page 5](#)
- [Junos OS Installation Packages on page 6](#)

Junos OS Editions



NOTE: Hardware platforms running Junos OS with the upgraded FreeBSD kernel employ a new naming scheme for software packages that does not recognize different major software package categories, such as domestic, world-wide, or Federal Information Processing Standard (FIPS). For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

Junos OS is released in the following editions:

- Domestic—Junos OS for customers in the United States and Canada, and for all other customers with a valid encryption agreement. This edition includes high-encryption capabilities such as ipsec and ssh for data leaving the router or switch.
- Export—Junos OS for all other customers. This edition does not include any high-encryption capabilities for data leaving the router or switch.
- Junos-FIPS—Junos OS that provides advanced network security for customers who need software tools to configure a network of Juniper Networks routers and switches in a Federal Information Processing Standards (FIPS) 140-2 environment. For more information about Junos-FIPS, see [“FIPS 140-2 Security Compliance” on page 5](#).

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)

FIPS 140-2 Security Compliance



NOTE: Hardware platforms running Junos OS with the upgraded FreeBSD kernel employ a new naming scheme for software packages that does not recognize different major software package categories, such as domestic, world-wide, or Federal Information Processing Standard (FIPS). For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

For advanced network security, a special version of Junos OS, called Junos-FIPS 140-2, is available. Junos-FIPS 140-2 provides customers with software tools to configure a network of Juniper Networks devices in a FIPS environment. FIPS support includes:

- Upgrade package to convert Junos OS to Junos-FIPS 140-2
- Revised installation and configuration procedures
- Enforced security for remote access
- FIPS user roles (Crypto Officer, User, and Maintenance)
- FIPS-specific system logging and error messages

- IPsec configuration for Routing Engine–to–Routing Engine communication
- Enhanced password creation and encryption

Junos-FIPS has special installation and configuration requirements. Installation procedures include downloading the FIPS software package from www.juniper.net. For detailed guidelines on how installation and configuration procedures differ between Junos OS and Junos-FIPS 140-2, see the [Secure Configuration Guide for Common Criteria and Junos-FIPS](#).



NOTE: Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the device, you cannot configure passwords unless they meet this standard.

Related Documentation

- [Understanding Junos OS with Upgraded FreeBSD Package Names](#) on page 22

Junos OS Installation Packages

The installation package is used to upgrade and downgrade from one release to another. When installed, the installation package completely reinstalls the software, rebuilds the Junos OS file system, and may erase system logs and other auxiliary information from the previous installation. The installation package does, however, retain the configuration files from the previous installation.

The following installation packages are available for download:



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Junos OS with upgraded FreeBSD has a different, simplified package naming convention. For more information, see [“Understanding Junos OS with Upgraded FreeBSD Package Names”](#) on page 22.

Installation Package	Description
jinstall*	Junos OS for M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers.
jinstall-ppc*	Junos OS for the ACX Series, MX80, and MX104 routers.
jinstall-ex*	Junos OS for the EX Series Ethernet Switch portfolio.

junos-juniper*	Junos-FIPS for the M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers. Once the package is installed on a device, you cannot revert back to the standard Junos OS installation without performing a software recovery procedure.
jinstall64*	64-bit Junos OS for the JCS1200 Route Reflector, TX Matrix Plus routers with 3D SIBs, and PTX Series Packet Transport Routers.
junos-srxsme*	Junos OS for all the branch SRX Series.
junos-srxentedge*	Junos OS for SRX1500
junos-srx5000*	Junos OS for SRX5400, SRX5600 and SRX5800.

**Related
Documentation**

- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)

Junos OS Package Names for EX Series Switches

You upgrade the Juniper Networks Junos operating system (Junos OS) on a Juniper Networks EX Series Ethernet Switch by copying a software package to your switch or another system on your local network, then install the new software package on the switch.

Two versions of a Junos OS image—a controlled version that supports Media Access Control Security (MACsec) and a domestic version that does not support MACsec—are available for EX Series switches. A domestic version of Junos OS is available for all EX Series switches; a controlled version of Junos OS is only available for EX Series switches on Junos OS releases that support MACsec. The domestic version of Junos OS on EX Series switches can be used on any switch in any geography. The controlled version of Junos OS contains encryption and is not available to customers in all geographies.



NOTE: The controlled version of Junos OS contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS is also subject to controls imposed under the laws of other countries.

If you have questions about acquiring the controlled version of Junos OS in your country, contact the Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.



NOTE: The domestic version of Junos OS on EX Series switches is intended for use on any switch in any worldwide location.

For most Junos packages on other Juniper Networks products, the domestic package is used for products installed in the United States and Canada only while an export package is used for products installed in any worldwide location.

domestic-signed indicates the domestic software package.

A domestic software package name is in the following format:

package-name-m.nZx.y-domestic-signed.tgz

A controlled software package name is in the following format:

package-name-m.nZx.y-controlled-signed.tgz

where:

- ***package-name*** is the name of the package—for example, ***jinstall-ex-4200***.
- ***m.n*** is the software release, with ***m*** representing the major release number and ***n*** representing the minor release number—for example, ***9.5***.
- ***Z*** indicates the type of software release, where ***R*** indicates released software and ***B*** indicates beta-level software.
- ***x.y*** represents the version of the major software release (***x***) and an internal tracking number (***y***)—for example, ***1.6***.
- ***domestic-signed*** indicates the domestic software package.
- ***controlled-signed*** indicates the controlled software package.

A sample EX Series software domestic package name is:

jinstall-ex-4200-9.5R1.6-domestic-signed.tgz

A sample EX Series controlled package name is:

jinstall-ex-4200-13.2X50-D15.3-controlled-signed.tgz

Related Documentation

- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
- [Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)
- [Downloading Software Packages from Juniper Networks on page 51](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

Software Naming Convention

All Junos OS conforms to the following naming convention:

package-release-edition-cfxxx-signed.comp

For example:

jinstall-9.2R1.8-domestic-signed.tgz

where:

- **package** is the name of the Junos OS package. For 64-bit Junos OS, the package name is **package64**.
- **cfxxx** designates the CompactFlash card size to use with the software. This value is optional.
- **signed** means that the software includes a digital signature for verification purposes. This value is not used with all software packages.

All SRX Series packages conform to the following naming convention:

junos-product-release-edition

For example:

junos-srxentedge-15.1X49-D30.3-domestic.tgz (for SRX1500)

junos-vsr-x-15.1X49-D30.3-domestic.tgz (for vSRX)

junos-srx5000-15.1X49-D30.3-domestic.tgz (for SRX5400, SRX5600, SRX5800)

junos-srxsme-15.1X49-D30.3-domestic.tgz (for SRX550M)

where:

- **product** means SRX Series product line.
- **edition** means Junos OS for customers in the United States and Canada, and for all other customers with a valid encryption agreement. This edition includes high-encryption capabilities such as IPsec and SSH for data leaving the device.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

Related Documentation

- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Junos OS Release Numbers on page 11](#)
- [FIPS 140-2 Security Compliance on page 5](#)
- [Junos OS Editions on page 5](#)

Software Naming Convention for SRX Series Devices

Typically, you upgrade your device software by downloading a software image to your device from another system on your local network. Using the J-Web user interface or the CLI to upgrade, the device downloads the software image, decompresses the image, and installs the decompressed software. Finally, you reboot the device, at which time it boots from the upgraded software. Junos OS is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.

An upgrade software package name for an SRX Series device is in the following format:

package-name-m.nZx-distribution.tgz

- **package-name**—Name of the package; for example, junos-srxsme.
- **m.n**—Junos OS release, with m representing the major release number and n representing the minor release number; for example, 10.0.
- **Z**—Type of Junos OS release; for example, R indicates released software, and B indicates beta-level software.

For more information, see “Junos OS Release Numbers” on page 11.



NOTE: Starting with Junos OS Release 12.1X44-D10, SRX Series devices follow a special naming convention for Junos OS releases. For more information, refer to the Knowledge Base article KB30092 at <http://kb.juniper.net/InfoCenter/index?page=home>.

- **x.y**—Junos OS build number and spin number; for example, 1.8.
- **distribution**—Area for which the Junos OS package is provided. It is domestic for the United States and Canada, and it is export for worldwide distribution.

The following package name is an example of an SRX Series device upgrade Junos OS package:

junos-srxentedge-15.1X49-D30.3-domestic.tgz

Related Documentation

- [FIPS 140-2 Security Compliance on page 5](#)
- [Junos OS Release Numbers on page 11](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)

Software Package Information Security

Junos OS software is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1), and Message Digest 5 (MD5) checksums. A package is installed only if the checksum within it matches the hash recorded in its corresponding file. Which checksum is used depends on the software version:

- Digital signatures are used when you upgrade or downgrade between Junos OS Release 7.0 and a later version.
- The SHA-1 checksum is used when you upgrade or downgrade between Junos OS Release 6.4 and a later version.
- The MD5 checksum is used when you upgrade or downgrade between Junos OS Release 6.3 or earlier and a later version.

Related Documentation

- [Installation Type Overview on page 41](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

Junos OS Release Numbers

The Junos OS release number represents a particular revision of the software that runs on a Juniper Networks routing platform, for example, Junos OS Release 14.1, 14.2, or 15.1. Each Junos OS release has certain new features that complement the software processes that support Internet routing protocols, control the device's interfaces and the device chassis itself, and allow device system management. On the Juniper Networks Support webpage, you download Junos OS for a particular Junos OS release number.

The following example shows how the software release number is formatted:

m.nZb.s

For example:

14.2R3.2

Where:

- *m* is the main release number of the product
- *n* is the minor release number of the product
- *Z* is the type of software release. The following release types are used:
 - *R*—FRS/Maintenance release software
 - *F*—Feature Velocity release software



NOTE: Feature velocity release was introduced in Junos OS Release 15.1.

- *B*—Beta release software

- *I*—Internal release software: Private software release for verifying fixes
- *S*—Service release software: Released to customers to solve a specific problem—this release will be maintained along with the life span of the underlying release
- *X*—Special (eXception) release software: Releases that follow a numbering system that differs from the standard Junos OS release numbering.

Starting with Junos OS Release 12.1X44-D10, SRX Series devices follow a special naming convention for Junos OS releases. For more information, refer to the Knowledge Base article KB30092 at

<http://kb.juniper.net/InfoCenter/index?page=home>.

- *b* is the build number of the product
 - if *b*=1: Software is the FRS release
 - if *b*>1: Software is a maintenance release

s is the spin number of the product

- For Service release software, the release number is added at the end. For example, 14.2R3-S4.4. Here S4 represents the 4th service release on top of 14.2R3 and is the 4th respin.



NOTE: Prior to Junos OS Release 11.4, the software release number format for service releases was same as other releases. For example, 10.4S4.2 represented the 4th service release and 2nd respin of 10.4.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see “[Understanding Junos OS with Upgraded FreeBSD Package Names](#)” on [page 22](#).

Related Documentation

- [Junos OS Installation Packages on page 6](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Junos OS Editions on page 5](#)

Installation Media

The installation media is used to recover a device from a software failure. The installation media repartitions the media and completely reinstalls Junos OS. No information from previous installations is retained during this installation. Thus, an initial configuration is required before the device can be put back into service. For more information about creating an initial configuration, see the *Getting Started Guide* for your device.



NOTE: Once you have rebuilt a device using the installation media, access to the device is restricted to the console port until the management port is configured during the initial configuration.

The following installation media files are available for download:

Installation Media	Description
floppy1-<release>*	Junos OS for the M40 router when you use the LS-120 external drive.
floppy2-<release>*	
install-media*	Junos OS for the ACX Series, M Series, MX Series, T Series, PTX Series Packet Transport Routers, TX Matrix, and TX Matrix Plus routers.



NOTE: Branch SRX Series Services Gateways are upgraded from loader prompt using USB or TFTP. For more details, see [“Installing Junos OS on SRX Series Devices Using a USB Flash Drive” on page 68](#) and [“Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server” on page 70](#).

Installation Bundles

The installation bundle can be used to downgrade or upgrade Junos OS between minor revisions (from Release 9.1 to Release 9.2, for example). When used, the installation bundle modifies only the files required for the upgrade or downgrade between versions.



NOTE: You should only use the installation bundle under direction of a Juniper Networks support representative.

The following installation bundle files are available for download:

Installation Bundle	Description
jbundle*	Junos OS for the ACX series, M Series, MX Series, T Series, PTX Series Packet Transport Routers, TX Matrix, and TX Matrix Plus routers.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names” on page 22](#).

Installation Modules

Installation modules are used to upgrade individual software modules in Junos OS. For example, you can upgrade only the Routing Engine software by installing the **jroute*** installation module.



NOTE: You should only use installation module files under the direction of a Juniper Networks support representative.

The following installation module files are available for download:

Installation Module	Description
jkernel*	The kernel and network tools package. This package contains the basic operating system files.
jbase*	The base package for Junos OS. This package contains additions to the operating system.
jroute*	The Routing Engine package. This package contains the Routing Engine software.
jpfe*	The Packet Forwarding Engine package. This package contains the PFE software.
jdocs*	The documentation package. This package contains the documentation set for the software.
jcrypto*	The encryption package. This package contains the domestic version of the security software.
jweb*	The J-Web package. This package contains the graphical user interface software for M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers.



NOTE: Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). Junos OS with upgraded FreeBSD has a new naming convention. For more information on this new naming convention, see [“Understanding Junos OS with Upgraded FreeBSD Package Names”](#) on page 22.

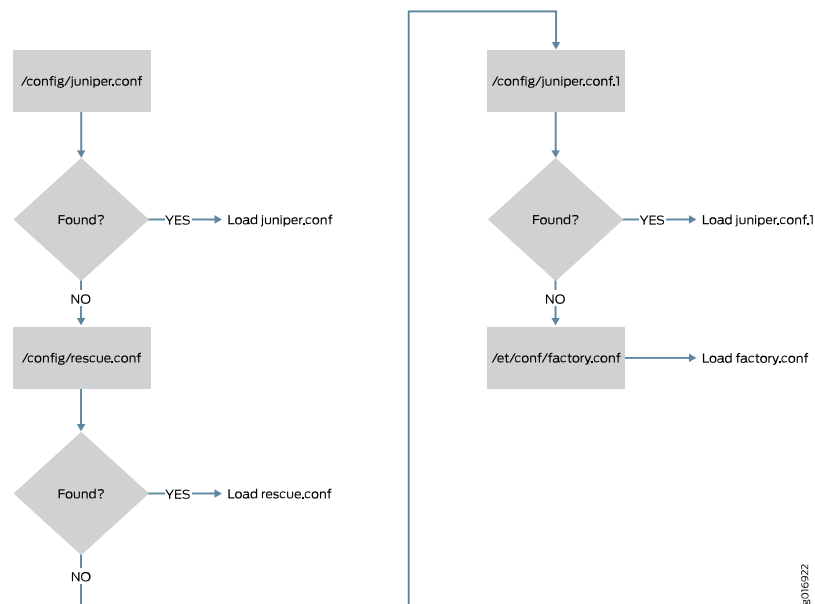
Configuration Files

All configuration settings for the device are handled in the configuration files on the device. These files are saved in the **/config** directory on the device.

Configuration File Selection Sequence

During the boot process, the device is configured based on a predefined configuration file. The device selects the configuration file based on the sequence shown in Figure 1.

Figure 1: Configuration Selection Sequence



1. **/config/juniper.conf**—Active configuration file.
2. **/config/rescue.conf**—Rescue configuration file. This file is created by the router or switch administrator.
3. **/config/juniper.conf.1**—First rollback configuration.
4. **/etc/config/factory.conf**—Default factory configuration file.

The **factory.conf** file is the initial device configuration file shipped with the system. All configuration settings are returned to the factory default, and access to the device is restricted to the console. For more information about setting up your device from the factory default configuration, see the specific hardware guide for your device.

For SRX Series Services Gateways running Junos Release 10.0 or later, the current operational Junos Software configuration is stored in a file named **juniper.conf**, and the last five committed configurations are stored in the files **juniper.conf.1** through **juniper.conf.5**. The rescue configuration is stored in a file named **rescue.conf**. These files

are located in the **/config** directory available on the flash drive of the SRX Series Services Gateway.

To list the configuration files, use the **file list /config** operational mode command.

```
user@host>file list / config
/config:
.snap/
idp-dfa-status.db
juniper.conf+.gz
juniper.conf.1.gz
juniper.conf.2.gz
juniper.conf.3.gz
juniper.conf.4.gz
juniper.conf.5.gz
juniper.conf.gz
juniper.conf.md5*
jwxd_initialized
license/
license-status.db
rescue.conf.gz
usage.db
usage.db.1344499761
```

Remote Storage of Configuration Files

Configuration files can be stored off the device. This can be helpful if the device encounters a software failure or other problem that forces you to restore the device's software. Once the software is restored, you can then reload the saved configuration file. For more information about restoring Junos OS, see [“Loading and Committing the Configuration File” on page 184](#).

When the configuration file is stored off the device, you can encrypt the configuration files using the Data Encryption Standard (DES) encryption algorithm.

Related Documentation

- [Installation Modules on page 14](#)

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- [Routing Engine and Packet Forwarding Engine on page 17](#)
- [Junos OS Processes on page 17](#)

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- Routing Engine—Provides three main functions:
 - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network
 - Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
 - Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

[Table 3](#) describes the primary Junos OS processes.

Table 3: Junos OS Processes

Process	Name	Description
Chassis process	chassisd	<p>Detects hardware on the system that is used to configure network interfaces.</p> <p>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</p> <p>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</p>
Ethernet switching process	eswd	<p>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces.</p> <p>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</p>
Forwarding process	pfem	<p>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</p>
Interface process	dcd	<p>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</p>
Management process	mgd	<p>Provides communication between the other processes and an interface to the configuration database.</p> <p>Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured.</p> <p>Interacts with the other processes when commands are issued through one of the user interfaces on the switch.</p> <p>If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</p>
Routing protocol process	rpd	<p>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</p>

Related Documentation

Understanding Junos OS with Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. Basing Junos OS on the newer kernel provides Junos OS with sophisticated processing, efficiency, and security features which do not then have to be reproduced in Junos OS.



NOTE: Upgrading to Junos OS Release 15.1 reformats the file system. Only specific files and directories are preserved unless precautions are taken. For details, see [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#).

Junos OS with an upgraded FreeBSD kernel provides a clean-slate implementation of Junos OS on top of a pristine (minimally modified) and current version of the FreeBSD OS.



NOTE: In Junos OS releases earlier than 15.1, the partition swap pages were counted as part of the memory file system partition. Using this method leaves 4 GB of memory as the maximum that is theoretically accessible when you are using a 32-bit image. However, when Junos OS with upgraded FreeBSD is run, the system only counts the actual partition size, which leaves around 3.4 GB of available physical address space, or only 3 GB of usable RAM. Therefore, we recommend you use a 64-bit image with Junos OS with upgraded FreeBSD.

The platforms currently running Junos OS with upgraded FreeBSD are listed in [Table 4](#).

Table 4: Upgraded FreeBSD Kernel Support by Hardware Platform

Platforms	CPU Type	Release Introduced
MX240, MX460, MX960, MX2010, MX2020	Intel	15.1
EX9200	Intel	15.1
QFX5200	Intel	15.1X53-D30
QFX10000 switches	Intel	15.1X53-D60

The major processing changes are as follows:

- Interactions between Junos OS and the upgraded FreeBSD kernel use well-established interfaces because Junos OS is now layered on a minimally modified and current version of FreeBSD.
- Symmetric multiprocessing (SMP) is enabled by default.

- FreeBSD provides a consistent runtime environment for all Junos OS platforms.

There are also major changes in file structures and software packages. These changes are as follows:

- New packages use XML description files instead of scripts.
- Hybrid packages are used to install legacy or replacement build images in the general form **junos-upgrade-x.tgz** where *x* is a variable such as **mx-x86-64-15.1-20150114** (the whole package name is **junos-upgrade-mx-x86-64-15.1-20150114.tgz**).
- Multiple package sets (a collection of installed packages) are stored on the router at the same time. Sets can be either active (the currently used set), pending (the set that should be used at the next reboot), or previous (a formerly active set). Non-recovery snapshots (but not recoverable image snapshots) are available for the package sets to preserve package content lists.

There is now a separate Operations, Administration, and Maintenance (OAM) volume (**oam**) distinct from the Junos OS volume (**junos**). This provides support for downgrades from replacement build images (that is, those using the upgraded FreeBSD kernel) to the legacy Junos OS with a different kernel. The OAM volume allows you to recover the Junos OS volume using recovery snapshots.

One major change is the distinction between recovery snapshots and non-recovery snapshots.

The major characteristics of the recovery snapshots are as follows:

- Recovery snapshots are full copies of the packages and configuration taken at the time the snapshot command is issued.
- Recovery snapshots reside on the OAM volume or USB medium.

The major characteristics of the non-recovery snapshots are as follows:

- Non-recovery snapshots are snapshots residing on the Junos OS volume that refer to the current running set of packages and a copy of the configuration at the time the snapshot command is issued.
- Non-recovery snapshots do not need to copy the whole Junos OS installation and so are very fast.
- Non-recovery snapshots can be requested as the boot image for the next reboot.

The upgraded FreeBSD kernel requires changes to several commands and statements and their related parameters. The new and changed actions are summarized in [Table 5](#). For details on the changes, see the topics covering the specific command or statement.

Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD

Command or Statement	Release Introduced	Change
request system snapshot delete <i>snapshot</i>	15.1	New action

Table 5: New and Changed Commands and Statements for Junos OS with Upgraded FreeBSD (continued)

Command or Statement	Release Introduced	Change
<code>request system snapshot recovery</code>	15.1	New action
<code>request system snapshot load <i>snapshot</i></code>	15.1	New action
<code>request system recover <i>volume</i></code>	15.1	New action: <i>volume</i> is either <code>/junos-volume</code> or <code>/oam-volume</code>
<code>request system snapshot</code>	15.1	Changed action
<code>show system snapshot</code>	15.1	Changed action
<code>request system reboot <i>media</i></code>	15.1	Changed action with new media options

The new FreeBSD kernel also requires that several commands and statements are now deprecated. In some cases, these commands and statements generate an error, and, in other cases, the result is appropriate for the new kernel. The deprecated commands and statements are summarized in [Table 6](#). For details, see the topics covering the specific command or statement.

Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD

Deprecated Command or Configuration Statement	Release Deprecated
Deprecated Command	
<code>request system partition abort</code>	15.1
<code>request system partition compact-flash</code>	15.1
<code>request system partition hard-disk</code>	15.1
<code>request system snapshot <config-partition></code>	15.1
<code>request system snapshot <root-partition></code>	15.1
<code>request system snapshot <slice></code>	15.1
<code>request system software delete-backup</code>	15.1
<code>request system software rollback <force></code>	15.1
<code>show system processes providers</code>	15.1
<code>show system snapshot <slice></code>	15.1
Deprecated Configuration Statement	

Table 6: Deprecated Commands and Statements for Junos OS with Upgraded FreeBSD (*continued*)

Deprecated Command or Configuration Statement	Release Deprecated
<code>set system mirror-flash-on-disk</code>	15.1

Related Documentation

- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 413](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 316](#)

Understanding Junos OS with Upgraded FreeBSD Package Names

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel (hereafter called Junos OS with upgraded FreeBSD). In releases earlier than Junos OS Release 15.1, software packages came in several major software package categories, such as domestic, worldwide, or Federal Information Processing Standard (FIPS). However, Junos OS with upgraded FreeBSD has a new naming convention: There is only one category, and FIPS, instead of being a separate category, is an option you select on installation. This topic describes the simplified naming convention for Junos OS with upgraded FreeBSD.

If your hardware platform is listed in the table in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#), then you must use the new package names for download and installation.

The components of the new package naming conventions are as follows:

- **Prefix**—This is **junos-install**. This prefix takes the place of the prefix **jinstall** and the bundle **bundle**. We still use the term *bundle* in the new package-naming convention.
- **Media keyword**—Added to the prefix, a media keyword is only used when the image is not for use with the **request system software add** command. Values for the **media** keyword include **usb** for images installed from a USB drive or **net** for images installed over a network; for example, the entire prefix of your package might be **junos-install-usb-**.
- **Platform**—This field indicates the major product group, such as **mx** or **qfx**.
- **Architecture**—This field indicates the CPU architecture of the platforms. Values include **x86** for Intel and **arm** for Advanced RISC Machines CPUs.
- **Application Binary Interface (ABI)**—This field indicates the “word length” of the CPU architecture. Values include **32** for 32-bit architectures and **64** for 64-bit architectures.
- **Release**—This field indicates the release number, such as **15.1R1.9**.
- **Edition**—The edition field is null (empty) for the standard (domestic) images. For jurisdictions with limits on dataplane encryption, this field is set to **limited**.

As before, all images are in tarred and gzipped (.tgz) format.



NOTE: There are no longer “export” worldwide images or separate FIPS images. The keyword “signed” no longer appears because all Junos OS images are signed for validation.

Examples of valid Junos OS software package names include the following:

- **junos-install-mx-x86-32-15.1R1.9.tgz**—An image for a supported MX Series platform outside the RTZ.
- **junos-install-mx-x86-32-15.1R1.9-limited.tgz**—An image for a supported MX Series platform used in the RTZ.
- **junos-install-usb-mx-x86-32-15.1R1.9.tgz**—An image stored on and installed from a USB drive for a supported MX Series platform outside the RTZ.

Because an upgrade to Junos OS with upgraded FreeBSD from a release earlier than Junos OS 15.1 restructures the disk file system, you can lose many configuration and log files that you might want to keep. Items that are essential can be preserved by moving or copying them to the **/var/preserve** directory.

**Related
Documentation**

- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)

Understanding Junos OS with Upgraded FreeBSD Snapshots

Starting with Junos OS Release 15.1, certain hardware platforms have two types of snapshots. These platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. The two types of snapshots have different content, locations, and purposes, so it is important that they are created and maintained properly. One major change is the distinction between recovery snapshots and non-recovery snapshots. The hardware platforms listed in the table in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19 have these two different types of snapshots.

Recovery snapshots are full copies of the packages and configuration taken at the time the snapshot command is issued. Recovery snapshots reside on the OAM volume or USB medium. Recovery snapshots take some time to complete because of the level of detail captured. Recovery snapshots can be used to recover the Junos OS volume. There is only ever one recovery snapshot on the system.

On the other hand, non-recovery snapshots are snapshots residing on the Junos OS volume that refer to the current running set of packages and a copy of the configuration at the time the snapshot command is issued. Non-recovery snapshots do not need to copy the whole Junos OS installation and so are very fast. They also consume little space, except for the **config.tgz** file. Non-recovery snapshots can be requested as the boot image for the next reboot. You can rename non-recovery snapshots and retain more than one. You rename the non-recovery snapshots with the same procedure used to rename any other file on the system.



NOTE: We recommend that you generate both a non-recovery and a recovery snapshot after you successfully upgrade to Junos OS with upgraded FreeBSD. These snapshots should be refreshed periodically.

Package sets relate to non-recovery and recovery snapshots. The **/active**, **/pending**, and **/previous** sets are all package sets. A non-recovery snapshot is also a package set in a sense, with the addition of a copy of the configuration at the time that the non-recovery snapshot is taken.

Packages that are no longer referenced by any package set or non-recovery snapshot are automatically deleted. We recommend deleting any old non-recovery snapshots after an upgrade so that old packages can be deleted and space recovered.

Some helpful commands for non-recovery snapshots are:

- **request system snapshot**—Use this command to create a non-recovery snapshot.
- **show system snapshot**—Use this command to list all the available non-recovery snapshots.
- **request system snapshot delete**—Use this command to delete a non-recovery snapshot.
- **request system snapshot recovery**—Use this command to create a recovery snapshot. You can use other parameters to determine the details of the recovery snapshot created. There is only ever one recovery snapshot on the system.

Related Documentation

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 413](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 316](#)
- [request system software validate on \(Junos OS with Upgraded FreeBSD\) on page 361](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names on page 22](#)
- [Understanding Junos OS with Upgraded FreeBSD Package Names for EX2300 and EX3400 Switches](#)
- [Understanding Junos OS with Upgraded FreeBSD Disk Volumes on page 24](#)

Understanding Junos OS with Upgraded FreeBSD Disk Volumes

Starting with Junos OS Release 15.1, certain hardware platforms have a new disk naming convention. These platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD.

The hardware platforms listed in the table in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19 have two volumes. The main device is the **/junos** volume and contains all of the software and files needed for the day-to-day running of the device. The compact flash drive is the **/oam** volume and stores recovery snapshot backup

information. In case of failure of the main drive (that is, the **/junos** volume), the **/oam** volume can be used to boot the system.

Because the **/junos** and **/oam** volumes have very different purposes, their content is different. Technically, these volumes are **dev/gpt/oam** and **dev/gpt/junos**, but the short forms (**/junos** and **/oam**) are used in this topic. Essentially, the **/junos** volume is used for the running device software and holds configuration information and logs, whereas the **/oam** volume is used for backup copies of everything needed in the event that the **/junos** volume fails.

The **/junos** volume contains a directory named **/packages/db** that has all the components present on the device, such as **os-kernel-123**, **os-kernel-456**, and so on. A sibling directory named **/package-sets** is also present. Package sets are an important concept in Junos OS with upgraded FreeBSD.

The **/package-sets** directory contains a package listing that gathers all the components of the running Junos OS into an XML format in the **/active** subdirectory. So **os-kernel-123** could be a component in the **/package-sets/active** subdirectory, but then **os-kernel-456** could not be in the same XML package. Package sets do not contain the kernel software itself (for example), but tell the device where to find the kernel component needed for the software package. The same kernel can be present in several package listings, but only one package can be active and running on the device at any given time.

There are several directories on the **/junos** volume where a particular software package listing can be found:

- **/previous**—The package set in this directory contains the list of all the components that ran on the device before the last upgrade.
- **/active**—The package set in this directory contains the list of all the software components currently running on the device.
- **/pending**—The package set in this directory contains the list of all the software components on the device that will run after the next reboot.



NOTE: After a successful reboot, the package set in the **/pending** directory becomes the active package set, and the package set in the **/active** directory becomes the previous set.

The **/junos** volume also contains non-recovery snapshots taken with the **request system snapshot** command. These types of snapshots are new to Junos OS with upgraded FreeBSD and cannot be used for recovery of a failed system. Non-recovery snapshots are a special type of package set that includes a copy of the configuration. There can be many non-recovery snapshots on the device, and the files can be renamed. Multiple non-recovery snapshots, essentially lists of software components and configuration files, can be helpful when major software or configuration changes are occurring and establishment of a known stable system baseline is required.

On the other hand, a recovery snapshot, created with the **request system snapshot recovery** command, is stored on the **/oam** volume and is always replaced when a new recovery snapshot is taken.

The **/oam** volume should contain all the information needed to reboot the system if there is a failure of the **/junos** volume and restore the system to the state running at the time of the failure. In order to perform this reboot, the **/oam** volume needs to have all of the information required to provide the system with a running configuration. This information is provided by the recovery snapshot, created with the **request system snapshot recovery** command. Although it can take a while to perform, the recovery snapshot establishes an **.izo** or **.iso** image of the running Junos OS.

In the case of a total failure of the **/junos** volume, the system can be booted from the **/oam** volume. The recovery snapshot can then restore the repaired system.

**Related
Documentation**

- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)

CHAPTER 2

Hardware Overview

- [Hardware Architecture Overview on page 27](#)
- [Hardware Overview \(ACX Series, M Series, MX Series, T Series, and TX Matrix Routers\) on page 28](#)
- [Hardware Overview of SRX Series Services Gateways on page 31](#)
- [Routing Engines and Storage Media Names \(ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers\) on page 32](#)
- [Storage Media Names for SRX Series Devices on page 34](#)
- [Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines on page 34](#)
- [Boot Sequence on SRX Series Devices on page 36](#)

Hardware Architecture Overview

Juniper Network routing platforms are made up of two basic routing components:

- **Routing Engine**—The Routing Engine controls the routing updates and system management.
- **Packet Forwarding Engine (PFE)**—The Packet Forwarding Engine performs Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding.

From a system administration perspective, you install the software onto the Routing Engine and during the installation, the appropriate software is forwarded to other components as necessary. Most Routing Engines include a CompactFlash card that stores Junos OS. On M Series Multiservice Edge Routers, MX240, MX480, and MX960 3D Universal Edge Routers, T Series Core Routers, and TX Matrix routers, the system also includes a hard disk or solid-state drive (SSD) that acts as a backup boot drive. PTX Series Packet Transport Routers and the TX Matrix Plus router include a solid state drive as a backup boot drive.



NOTE: The MX80 router is a single-board router with a built-in Routing Engine and single Packet Forwarding Engine. On an MX80 router, Junos OS is stored on dual, internal NAND flash devices. These devices provide the same functionality as a CompactFlash card and hard disk or solid-state drive (SSD).



NOTE: The ACX Series router is a single board router with a built-in Routing Engine and one Packet Forwarding Engine. The ACX router supports dual-root partitioning, which means that the primary and backup Junos OS images are kept in two independently bootable root partitions. If the primary partition becomes corrupted, the system remains fully functional by booting from the backup Junos OS image located in the other root partition.

On routing platforms with dual Routing Engines, each Routing Engine is independent with regard to upgrading the software. To install new software on both Routing Engines, you need to install the new software on each Routing Engine. On platforms with dual Routing Engines configured for high availability, you can use the unified in-service software upgrade procedure to upgrade the software. For more information about this procedure, see the [High Availability Feature Guide for Routing Devices](#).

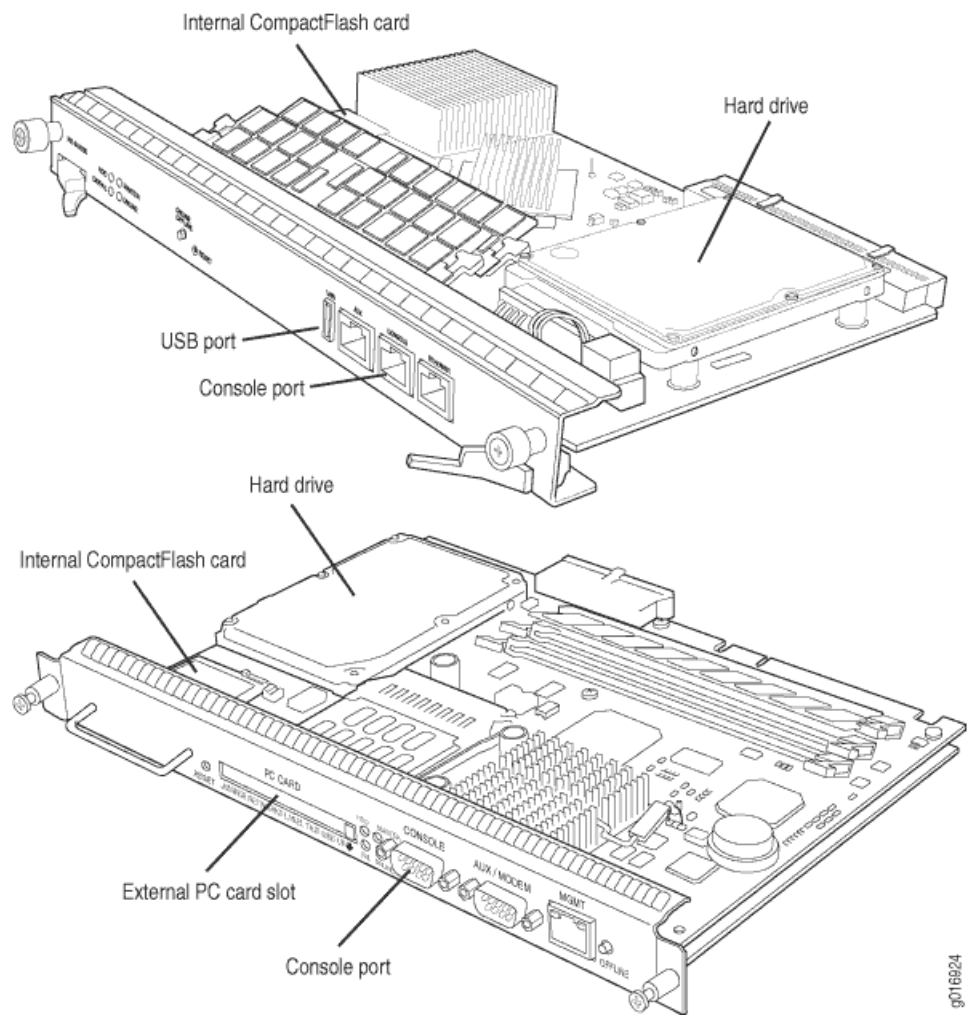
**Related
Documentation**

- [Dual-Root Partitioning ACX Series Universal Access Routers Overview](#)

[Hardware Overview \(ACX Series, M Series, MX Series, T Series, and TX Matrix Routers\)](#)

[Figure 2](#) shows examples of Routing Engines.

Figure 2: Routing Engines



The ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers include the following:

- [System Memory on page 29](#)
- [Storage Media on page 30](#)

System Memory

Starting with Junos OS Release 9.0, all routing platforms require a minimum of 512 MB of system memory on each Routing Engine. All M7i and M10i routers delivered before December 7, 2007, had 256 MB of memory. These routers require a system memory upgrade before you install Junos OS Release 9.0 or a later release. To determine the amount of memory currently installed on your system, use the **show chassis routing-engine** command in the command-line interface (CLI).

For more information about upgrading your M7i or M10i router, see the Customer Support Center JTAC Technical Bulletin PSN-2007-10-001:

<https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2007-10-001&actionBtn=Search>.

ACX2000 routers are shipped with 2 GB of memory and ACX1000 routers with 1 GB of memory.

Storage Media

Except for the ACX Series, MX80 routers, MX104 routers, the M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers use the following media storage devices:

- CompactFlash card—The CompactFlash card is typically the primary storage device for most routers.



NOTE: M7i and M10i routers using RE-400 are not delivered from the factory with the CompactFlash card installed. In this case, the hard disk is the primary and only boot device. The M7i and M10i routers with RE-400 can be upgraded to include the CompactFlash card.

- Hard disk or solid-state drive—For most routers,, a hard disk or solid-state drive is the secondary boot device. When the CompactFlash card is not installed on the router, the hard disk or the solid-state drive becomes the primary boot device. The hard disk or solid-state drive is also used to store system log files and diagnostic dump files.
- Emergency boot device—Depending on the router, the emergency boot device can be a PC card, a USB storage device, or an LS-120 floppy disk.

On MX80 routers, the internal NAND flash devices (first *da0*, then *da1*) act as the primary and secondary boot devices.

On ACX Series routers, the internal NAND flash devices (first *da0s1*, then *da0s2*) act as the primary and secondary boot devices.

Emergency boot devices can be used to revive a routing platform that has a damaged Junos OS. When an emergency boot device is attached to the router, the router attempts to boot from that device before it boots from the CompactFlash card, solid-state drive (SSD), or hard disk.

On an ACX Series router, the emergency boot device is a USB storage device.

On MX104 routers, the internal NAND flash device (**da0**) mounted on the internal eUSB card acts as the primary boot and storage device. On MX104 routers, the emergency boot device is a USB storage device that is plugged into one of the USB ports in the front plate.

When booting from an emergency boot device, the router requests a boot acknowledgment on the console interface. If you enter yes, the emergency boot device repartitions the primary boot device and reloads Junos OS onto the primary boot device. After the loading is complete, the routing platform requests that you remove the

emergency boot device and reboot the system. After the reboot is complete, you must perform an initial configuration of the router before it can be used on your network.

Hardware Overview of SRX Series Services Gateways

SRX Series Device Overview

Figure 3 shows an example of an SRX345 device.

Figure 3: SRX345 Device Front Panel

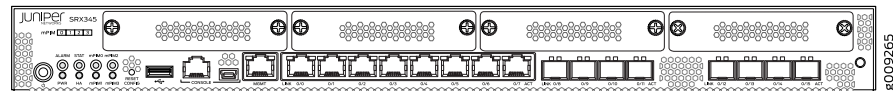


Figure 4 shows an example of an SRX1500 device.

Figure 4: SRX1500 Device Front Panel

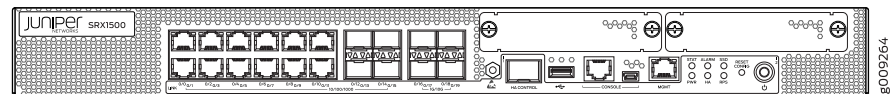
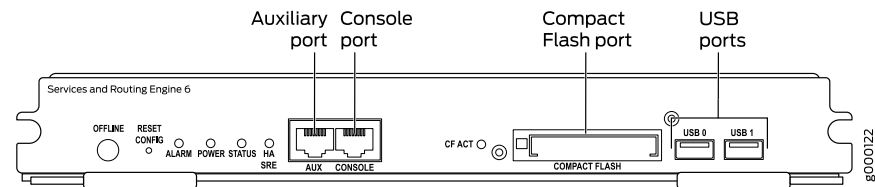


Figure 5 shows an example of an SRX5800 device Routing Engine.

Figure 5: SRX5800 Device Routing Engine



System Memory

The amount of free disk space necessary to upgrade a device with a new version of Junos OS can vary from one release to another for different SRX Series devices. Check the Junos OS software version you are installing to determine the free disk space requirements.

To determine the amount of free disk space on the device, issue the **show system storage detail** command. The command output displays statistics about the amount of free disk space in the device file systems.

Storage Media

The SRX300, SRX320, SRX340, 345 Services Gateway can boot from the following storage media (in the order of priority):

- Internal NAND flash device mounted on the internal eUSB card (default; always present)
- USB storage key (alternate)

The SRX550M Services Gateway can boot from the following storage media (in the order of priority):

- CompactFlash (default; always present)
- USB storage key (alternate)

SRX1500 device use the following media storage devices:

- Internal eSATA flash disk (default; always present)
- SSD Card

SRX5400, SRX5600, SRX5800 devices use the following media storage devices:

- The CompactFlash card in the Routing Engine
- The hard disk in the Routing Engine



NOTE: You can also use a Junos OS image stored on a USB flash drive that you insert into the Routing Engine faceplate.

**Related
Documentation**

- [Boot Sequence on SRX Series Devices on page 36](#)
- [Verifying PIC Combinations on page 269](#)

Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)

Table 7 specifies the storage media names by Routing Engine. The storage media device names are displayed when the router boots.

Table 7: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers)

Routing Engine	CompactFlash Card	Hard Disk	Solid State Drive	Removable Media Emergency Boot Device
RE-400-768 (RE5)	ad0	ad1	No	ad3
RE-600-2048 (RE3)	ad0	ad1	No	ad3
RE-850-1536 (RE-850)	ad0	ad1	No	ad3
RE-A-1000-2048 (RE-A-1000)	ad0	ad2	No	da0

Table 7: Routing Engines and Storage Media Names (ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers) (continued)

Routing Engine	CompactFlash Card	Hard Disk	Solid State Drive	Removable Media Emergency Boot Device
RE-A-1800x2 (RE-A-1800)	ad0	No	Yes SSD1: ad1 SSD2: ad2	da0
RE-S-1300-2048 (RE-S-1300)	ad0	ad2	No	da0
RE-S-1800x2 RE-S-1800x4 (RE-S-1800)	ad0	No	Yes SSD1: ad1 SSD2: ad2	da0
RE-B-1800X1-4G-S	ad0	No	Yes SSD1: ad1	da0
RE-1600-2048 (RE4)	ad0	ad1	No	ad3 and ad4
RE-A-2000-4096 (RE-A-2000)	ad0	ad2	No	da0
RE-S-2000-4096 (RE-S-2000)	ad0	ad2	No	da0
RE-MX-104	No	da0	No	da1 and da2
RE-DUO-C2600-16G (RE-DUO-2600)	ad0	No	ad1	da0
RE-DUO-C1800-8G- (RE-DUO-1800)	ad0	No	ad1	da0
RE-DUO-C1800-16G	ad0	No	ad1	da0
RE-JCS1200-1x2330	da0	da1	No	da2



NOTE: On MX80 routers, the Routing Engine is a built-in device and has no model number. The dual internal NAND flash devices are *da0* and *da1*. The USB storage device is *da2*.



NOTE: On ACX Series routers, the Routing Engine is a built-in device, which does not have a model number. The dual internal NAND flash devices are da0s1 and da0s2. The USB storage device is da0s2a. Use the `show chassis hardware models` command to obtain the field-replaceable unit (FRU) model number—for example, ACX2000BASE-DC for the ACX2000 router.

To view the storage media currently available on your system, use the CLI **show system storage** command. For more information about this command, see the *CLI User Guide*.

Related Documentation

- *Supported Routing Engines by Router*
- *Routing Engine Specifications*
- *RE-S-1300 Routing Engine Description*
- *RE-S-2000 Routing Engine Description*
- *RE-S-1800 Routing Engine Description for MX Series*
- *JCS1200 Routing Engine Description*

Storage Media Names for SRX Series Devices

Table 8 specifies the storage media names used by the SRX Series devices. The storage media device names are displayed as the device boots.

Table 8: Storage Media Names

Device	Internal CompactFlash Card	USB Storage Media Devices
SRX Series device	da0	da1

To view the storage media currently available on your system, use the CLI **show system storage** command.

Related Documentation

- [Hardware Overview of SRX Series Services Gateways on page 31](#)
- [Boot Sequence on SRX Series Devices on page 36](#)

Boot Sequence on M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series Devices with Routing Engines



NOTE: For information about which Routing Engines are supported by each device, see http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/general/routing-engine-m-mx-t-series-support-by-chassis.html.

The M Series, MX Series (except for the MX80 routers and the MX104 routers), T Series, and TX Matrix routers with a Routing Engine that has a hard disk attempt to boot from the storage media in the following order:

1. Removable media emergency boot device, such as a PC Card (if present)
2. CompactFlash card (if present)
3. Hard disk

The M Series and MX Series with a Routing Engine that has a solid-state drive (SSD) attempt to boot from the storage media in the following order:

1. USB media emergency boot device (if present)
2. CompactFlash card
3. Solid-state drive (SSD) in the SSD slot 1 or SSD slot 2 (if present)

MX80 routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. Dual, internal NAND flash device (first *da0*, then *da1*)

MX104 routers attempt to boot from the storage media in the following order:

1. USB storage media device
2. Internal NAND flash device (**da0**)

The T series routers with a Routing Engine that has a solid-state drive (SSD), and TX Matrix Plus routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. CompactFlash card (if present)
3. Solid-state drive (SSD) in the Disk 1 slot (if present)



NOTE: The Disk 2 slot is not currently supported.

4. Storage media available on the LAN

The ACX Series routers attempt to boot from the storage media in the following order:

1. USB storage media device
2. Dual, internal NAND flash device (first **da0s1**, then **da0s2**)

The PTX Series Packet Transport Routers attempt to boot from the storage media in the following order:

1. USB media emergency boot device
2. CompactFlash card

3. Solid-state drive (SSD) in the Disk 1 slot (if present)
4. Storage media available on the LAN



NOTE: Do not insert an emergency boot device during normal operations. The router does not operate normally when it is booted from an emergency boot device.

If the router boots from an alternate boot device, Junos OS displays a message indicating this when you log in to the router. For example, the following message shows that the software booted from the hard disk (`/dev/ad1s1a`):

```
login: username
Password: password
Last login: date on terminal
```

```
--- Junos 8.0 R1 built date
```

```
---
```

```
--- NOTICE: System is running on alternate media device (/dev/ad2s1a).
```

This situation results when the router detects a problem with the primary boot device—usually the CompactFlash card—that prevents it from booting, and consequently boots from the alternate boot device (the hard disk drive). When this happens, the primary boot device is removed from the list of candidate boot devices. The problem is usually a serious hardware error. We recommend you contact the Juniper Networks Technical Assistance Center (JTAC).



NOTE: On MX104 routers, if the router boots from an alternate boot device, Junos OS does not display any message indicating this when you log in to the router.

When the router boots from the alternate boot device, the software and configuration are only as current as the most recent **request system snapshot** command. However, if the **mirror-flash-on-disk** command was enabled, then the hard disk drive contains a synchronized, mirror image of the compact flash drive and therefore the current software and configuration.

Related Documentation

- *Routing Engine Specifications*

Boot Sequence on SRX Series Devices

On SRX Series devices, the device attempts to boot from the storage media in the following order:

- Internal CompactFlash card
- Internal eSATA flash disk (for SRX1500 devices)

- USB storage media device

**Related
Documentation**

- [Hardware Overview of SRX Series Services Gateways on page 31](#)
- [Storage Media Names for SRX Series Devices on page 34](#)

PART 2

Installing Junos Software

- [Installation Overview on page 41](#)
- [Performing a Standard or Change Category Installation on page 47](#)
- [Configuring Zero Touch Provisioning on page 73](#)
- [Configuring Automatic Installation of Configuration Files on page 81](#)
- [Configuring Dual-Root Partitions for High Availability on page 95](#)
- [Upgrading Software on page 115](#)
- [Booting a Device Using a System Snapshot on page 159](#)
- [Performing a Recovery Installation on page 165](#)
- [Reinstalling Software on page 187](#)
- [Downgrading Software on page 209](#)
- [Rebooting or Halting Software Processes on a Device on page 213](#)

CHAPTER 3

Installation Overview

- [Installation Type Overview on page 41](#)
- [Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers on page 42](#)
- [Installation Categories on SRX Series Devices on page 43](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

Installation Type Overview

The three types of installations used to upgrade or downgrade your routing platform are standard installation, category change, and recovery. The standard installation is the standard method of upgrading and downgrading the software. Use a category change installation when you are moving from one software category to another; for example, if you are changing the device from using the standard Junos OS to the Junos-FIPS category. Perform a recovery installation when the software on the device is damaged or otherwise unable to accommodate a software upgrade or downgrade.

Standard Installation

A standard installation is the typical method used to upgrade or downgrade software on the server. This method uses the installation package that matches the installation package already installed on the system.

For information on the different installation packages available, see [“Junos OS Installation Packages” on page 6](#).

Category Change Installation

The category change installation process is used to move from one category of Junos OS to another on the same router; for example, moving from a Junos OS standard installation to a Junos-FIPS installation. When moving from one installation category to another, you need to be aware of the restrictions regarding this change.



NOTE: Juniper Networks does not support using the `request system software rollback` command to restore a different installation category on the device. When installing a different Junos OS category on a device, once the installation is complete, you should execute a `request system snapshot` command to delete the backup installation from the system.

Recovery Installation

A recovery installation is performed to repair a device with damaged software or a condition that prevents the upgrade, downgrade, or change in installation category of the software.

For example, you may need to perform a recovery installation to change a device's software category from Junos-FIPS to standard Junos OS.

Related Documentation

- [Junos OS Installation Packages on page 6](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

Installation Categories on the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus Routers

The following installation categories are available with the ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus routers:

- Standard Junos OS, domestic—`jinstall-<release>-domestic-signed.tgz`

This software includes high-encryption capabilities for data leaving the router. Because of U.S. government export restrictions, this software can only be installed on systems within the United States and Canada. For all other customers, a valid encryption agreement is required to use this software edition. Furthermore, no router can be shipped out of the United States or Canada without the domestic edition first being overwritten by the export edition. There are no current system-enforced restrictions when you install this software category.

- Standard Junos OS, export—`jinstall-<release>-export-signed.tgz`

This software does not include high-encryption capabilities. It can be installed on any system worldwide. There are no current system-enforced restrictions when you install this software category.

- Junos-FIPS—`junos-juniper-<release>-domestic-signed.tgz` and `junos-juniper-<release>-fips-signed.tgz`

The Junos-FIPS OS base provides customers with the software tools to configure the router for use within a Federal Information Processing Standards (FIPS) environment. Once you have installed this software category onto a router, you cannot install a different software category on the router using the `request system software add` command. When attempting to install a different Junos OS category package on the router, you receive the following warning message:

WARNING: Package `jinstall-<release>-<edition>-signed` is not compatible with this system.

WARNING: Please install a supported package (`junos-juniper-*.tgz`).

To return to a standard Junos OS category installation, you must perform a system recovery installation of the software. All configuration files, logs, and other data files on the server are overwritten during a recovery installation.

For more information about Junos-FIPS OS base, see [“FIPS 140-2 Security Compliance” on page 5](#).



NOTE: When you install a Junos OS installation package, the previous installation is maintained as a backup installation. You should issue a `request system software snapshot` command to overwrite the backup files any time you change software categories on a router. This is mandatory if the router is to be shipped outside of the United States or Canada after the Export edition of Junos OS has been installed. There are no current system-enforced restrictions when you install this software category.

Installation Categories on SRX Series Devices

The following installation categories are available with the SRX Series devices:

- Junos OS, domestic—`junos-srxsme-<release>-domestic.tgz` for SRX Series devices. .

This software includes high-encryption capabilities for data leaving the router. Because of U.S. government export restrictions, this software can only be installed on systems within the United States and Canada. For all other customers, a valid encryption agreement is required to use this software edition. Furthermore, no router can be shipped out of the United States or Canada without the domestic edition first being overwritten by the export edition. There are no current system-enforced restrictions when you install this software category.

- Junos OS, export—`junos-srxsme-<release>-export.tgz` for SRX Series devices.

This software does not include high-encryption capabilities. It can be installed on any system worldwide. There are no current system-enforced restrictions when you install this software category.

Related Documentation

- [Installation Type Overview on page 41](#)
- [Software Package Information Security on page 11](#)
- [Software Naming Convention for SRX Series Devices on page 10](#)

Understanding Software Installation on EX Series Switches

A Juniper Networks EX Series Ethernet Switch is delivered with the Juniper Networks Junos operating system (Junos OS) preinstalled. As new features and software fixes become available, you must upgrade your software to use them. You can also downgrade Junos OS to a previous release.

This topic covers:

- [Overview of the Software Installation Process on page 44](#)
- [Software Package Security on page 44](#)
- [Installing Software on a Virtual Chassis on page 45](#)
- [Installing Software on Switches with Redundant Routing Engines on page 45](#)
- [Installing Software Using Automatic Software Download on page 45](#)
- [Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick on page 46](#)
- [Installing Software on an EX2300 or EX3400 Switch on page 46](#)
- [Troubleshooting Software Installation on page 46](#)

Overview of the Software Installation Process

An EX Series switch is delivered with a domestic version of Junos OS preinstalled. When you connect power to the switch, it starts (boots) from the installed software.

You upgrade Junos OS on an EX Series switch by copying a software package to your switch or another system on your local network, then use either the J-Web interface or the command-line interface (CLI) to install the new software package on the switch. Finally, you reboot the switch; it boots from the upgraded software. After a successful upgrade, you should back up the new current configuration to a secondary device. You should follow this procedure regardless of whether you are installing a domestic or controlled Junos OS package.

During a successful upgrade, the upgrade package removes all files from `/var/tmp` and completely reinstalls the existing software. It retains configuration files, and similar information, such as secure shell and host keys, from the previous version. The previous software package is preserved in a separate disk partition, and you can manually revert back to it if necessary. If the software installation fails for any reason, such as loss of power during the installation process, the system returns to the originally active installation when you reboot.

Software Package Security

All Junos OS releases are delivered in signed packages that contain digital signatures to ensure official Juniper Networks software. For more information about signed software packages, see the [Junos OS Installation and Upgrade Guide](#).

Installing Software on a Virtual Chassis

You can connect individual EX Series switches together to form one unit and manage the unit as a single device, called a Virtual Chassis. The Virtual Chassis operates as a single network entity composed of member switches. Each member switch in a Virtual Chassis must be running the same version of Junos OS. See *EX Series Virtual Chassis Software Features Overview* for a list of switches that can be used in a Virtual Chassis.

For ease of management, a Virtual Chassis provides flexible methods to upgrade software releases. You can deploy a new software release to all member switches of a Virtual Chassis or to only a particular member switch.

You can also upgrade the software on an EX4200, EX4500, mixed EX4200 and EX4500, and EX8200 Virtual Chassis using nonstop software upgrade (NSSU). NSSU takes advantage of graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) to ensure no disruption to the control plane during the upgrade. You can minimize disruption to network traffic by defining link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards (on EX8200 Virtual Chassis) or on different members (on EX4200, EX4500, mixed EX4200 and EX4500 Virtual Chassis). During an NSSU, the line cards and Virtual Chassis members are upgraded one at a time, so that traffic continues to flow through the other line cards or members while that line card or member is being upgraded.

Installing Software on Switches with Redundant Routing Engines

You can install software on a switch with redundant Routing Engines in one of two ways:

- Perform an NSSU—An NSSU upgrades both Routing Engines with a single command and with a minimum of network disruption. An NSSU takes advantage of GRES and NSR to ensure no disruption to the control plane. You can minimize disruption to network traffic by defining LAGs such that the member links of each LAG reside on different line cards. The line cards are upgraded one at a time, so that traffic continues to flow through the other line cards while a line card is being upgraded.

You cannot use NSSU to downgrade the software running on a switch.

For more information about NSSU, see [“Understanding Nonstop Software Upgrade on EX Series Switches” on page 123](#). See *EX Series Switch Software Features Overview* for a list of switches that support NSSU.

- Upgrade each Routing Engine manually—You can perform a Junos OS installation on each Routing Engine separately, starting with the backup Routing Engine. You can use this procedure to downgrade the software running on a switch. See *Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*.

Installing Software Using Automatic Software Download

The automatic software download feature uses the DHCP message exchange process to download and install software packages. Users can define a path to a software package on the DHCP server and then the DHCP server communicates this path to EX Series switches acting as DHCP clients as part of the DHCP message exchange process. The DHCP clients that have been configured for automatic software download receive these

messages and, when the software package name in the DHCP server message is different from that of the software package that booted the DHCP client switch, download and install the software package. See [“Upgrading Software by Using Automatic Software Download”](#) on page 129.

Autoinstalling a Configuration File on an EX2200 or EX3300 Switch from a Disk-on-Key USB Memory Stick

You can use an autoinstallation process to configure the software on an EX2200 or EX3300 switch. You can use a configuration file that is in either text format or XML format. If you want to use an XML-formatted file, you use a Junos Space platform to create the configuration file. You place the configuration file on a Disk-on-Key USB memory stick.

Installing Software on an EX2300 or EX3400 Switch

Before installing software on an EX2300 or EX3400 switch:

- Ensure that at least 620 MB of disk space is available in the system before downloading the software installation package to the `/var/tmp` directory. Use the command **show system storage** to get details of the available space.
- If the space available is inadequate, use the command **request system storage cleanup**. Additionally, you can manually delete any other log or unwanted files from the `/var/tmp` or `/var/log` directories.

You can now follow the procedure in *Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)* to complete the software installation.

Troubleshooting Software Installation

If Junos OS loads but the CLI is not working for any reason, or if the switch has no software installed, you can use the recovery installation procedure to install the software on the switch. See [“Troubleshooting Software Installation”](#) on page 265.



NOTE: You can also use this procedure to load two versions of Junos OS in separate partitions on the switch.

Related Documentation

- [Downloading Software Packages from Juniper Networks on page 51](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
- [Installing Software on an EX Series Switch with Redundant Routing Engines \(CLI Procedure\)](#)
- [Understanding Nonstop Software Upgrade on EX Series Switches on page 123](#)

CHAPTER 4

Performing a Standard or Change Category Installation

- [Checking the Current Configuration and Candidate Software Compatibility on page 47](#)
- [Determining the Junos OS Version on page 48](#)
- [Downloading Software on page 48](#)
- [Downloading Software Packages from Juniper Networks on page 51](#)
- [Understanding Download Manager for SRX Series Devices on page 51](#)
- [Understanding the Console Port on page 53](#)
- [Backing Up the Existing Installation on Routers on page 55](#)
- [Backing Up the Current Installation on SRX Series Devices on page 56](#)
- [Installing the Software Package on a Router with a Single Routing Engine on page 57](#)
- [Installing the Software Package on a Router with Redundant Routing Engines on page 58](#)
- [Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Registering the EX Series Switch with the J-Web Interface on page 66](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 66](#)
- [Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 69](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)

Checking the Current Configuration and Candidate Software Compatibility

When you upgrade or downgrade Junos OS, we recommend that you include the **validate** option with the **request system software add** command to check that the candidate software is compatible with the current configuration. By default, when you add a package with a different release number, the validation check is done automatically.



NOTE: On an ACX Series router, you must ensure that the primary and backup partitions are synchronized after an upgrade by issuing the `request system snapshot` command.

**Related
Documentation**

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)
- [request system snapshot \(SRX Series\) on page 331](#)
- [request system software add \(Maintenance\) on page 344](#)

Determining the Junos OS Version

To determine which software packages are running on the device and to get information about these packages, use the **show version** operational mode command at the top level of the command-line interface (CLI).



NOTE: The `show version` command does not show the software category installed, only the release number of the software.

**Related
Documentation**

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Downloading Software

You can download the software in one of two ways:

- [Downloading Software with a Browser on page 49](#)
- [Downloading Software Using the Command-Line Interface on page 49](#)

Downloading Software with a Browser

You download the software package you need from the Juniper Networks Support website at <http://www.juniper.net/support/>.



NOTE: To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>.

To download the software:

1. In a browser, go to <http://www.juniper.net/support/>.
The Support page opens.
2. In the Download Software section, select the software version to download.
Depending on your location, select Junos Canada and US, or Junos Worldwide.
3. Select the current release to download.
4. Click the Software tab and select the Junos OS installation package to download.
A dialog box opens.
5. Save the file to your system. If you are placing the file on a remote system, you must make sure that the file can be accessible by the router or switch using HTTP, FTP, or scp.

Downloading Software Using the Command-Line Interface

Download the software package you need from the Juniper Networks Support website at <http://www.juniper.net/support/>, and place the package on a local system. You can then transfer the downloaded package to the device using either the router or switch command-line interface, or the local system command-line interface.



NOTE: To access the download section, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>.

Before you transfer the software package, ensure that the FTP service is enabled on the device.

Enable the FTP service using the **set system services ftp** command:

```
user@host# set system services ftp
```

To transfer the software package using the device command-line interface:

1. From the router or switch command line, initiate an FTP session with the local system (host) where the package is located using the **ftp** command:

```
user@host> ftp host
```

host is the Hostname or address of the local system.

2. Log in with your customer support–supplied username and password:

```
User Name: username
331 Password required for username.
Password: password
```

Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **get** command:

```
user@host> get installation-package
```

Following is an example of an *installation-package* name:

jinstall-9.2R1.8–domestic-signed.tgz

4. Close the FTP session using the **bye** command:

```
user@host> bye
Goodbye
```

To transfer the package using the local system command-line interface:

1. From the local system command line, initiate an FTP session with the device using the **ftp** command:

```
user@host> ftp host
```

host is the Hostname or address of the router or switch.

2. Log in with your customer support–supplied username and password:

```
User Name: username
331 Password required for username.
Password: password
```

Once your credentials have been validated, the FTP session opens.

3. Navigate to the software package location on the local system, and transfer the package using the **put** command:

```
user@host> put installation-package
```

Following is an example of an *installation-package* name:

jinstall-9.2R1.8–domestic-signed.tgz

4. Close the FTP session using the **bye** command:

```
user@host> bye
Goodbye
```

**Related
Documentation**

- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)

- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Downloading Software Packages from Juniper Networks

You can download Junos OS packages from the Juniper Networks website to upgrade software on your EX Series switch.

Before you begin to download software upgrades, ensure that you have a Juniper Networks Web account and a valid support contract. To obtain an account, complete the registration form at the Juniper Networks website: <https://www.juniper.net/registration/Register.jsp>.

To download software upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. For EX Series, there are not separate software packages for Canada the U.S. and other locations. Therefore, select **Canada and U.S. Version** regardless of your location:
 - <https://www.juniper.net/support/downloads/junos.html>
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using the J-Web interface or the CLI, select the appropriate software package for your application. See “[Junos OS Package Names for EX Series Switches](#)” on page 7.
4. Download the software to a local host or to an internal software distribution site.

Related Documentation

- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

Understanding Download Manager for SRX Series Devices

This topic includes the following sections:

- [Overview on page 51](#)
- [Using Download Manager to Upgrade Junos OS on page 52](#)
- [Handling Errors on page 52](#)
- [Considerations on page 53](#)

Overview

This download manager feature facilitates download of large files over low-bandwidth links. It enables you to download large Junos OS packages over low-bandwidth/flaky links so that the system can be upgraded. This feature allows you to download multiple

files while monitoring their status and progress individually. It takes automatic action when required and displays status information when requested.

This feature provides the following functions:

- Bandwidth-limited downloads
- Scheduled downloads
- Automatic resume on error
- Automatic resume on reboot



NOTE: This feature supports only the FTP and HTTP protocols.

Using Download Manager to Upgrade Junos OS

The download manager acts as a substitute for the FTP utility. You can use the download manager CLI commands for all the functions where you previously used the FTP utility.

The download manager requires the following:

- FTP or HTTP server with a Junos OS image
- Server that is reachable from the device being upgraded

The download manager consists of the following CLI commands:

1. To download the Junos OS image to your device, use the **request system download start** command (set a bandwidth limit, if required). The file is saved to the **/var/tmp** directory on your device.

You can continue to use the device while the download runs in the background.
2. Use the **show system download** command to verify that the file has been downloaded. The command displays the state as "completed" when the downloaded file is ready to be installed.
3. Use the **request system software add** command to install the downloaded image file from the **/var/tmp** directory.

Handling Errors

If you encounter any problem with a download, use the **show system download id** command to obtain details about the download.

Table 9 lists the output fields for the **show system download** command. Use this information to diagnose problems. Output fields are listed in the approximate order in which they appear.

Table 9: show system download Output Fields

Output Field	Description
Status	State of the download.
Creation Time	Time the start command was issued.
Scheduled Time	Time the download was scheduled to start.
Start Time	Time the download actually started (if it has already started).
Retry Time	Time for next retry (if the download is in the error state).
Error Count	Number of times an error was encountered by this download.
Retries Left	Number of times the system will retry the download automatically before stopping.
Most Recent Error	Message indicating the cause of the most recent error.

Considerations

- When no download limit is specified for a specific download or for all downloads, a download uses all available network bandwidth.
- Because the download limit that you set indicates an average bandwidth limit, it is possible that certain bursts might exceed the specified limit.
- When a download from an HTTP server fails, the server returns an HTML page. Occasionally, the error page is not recognized as an error page and is downloaded in place of the Junos image file.
- Remote server logins and passwords are stored by the download manager for the duration of a download. To encrypt these credentials provided along with the login keyword, define an encryption key with the **request system set-encryption-key** command. Any changes to encryption settings while download is in progress can cause the download to fail.
- A download command issued on a particular node in a chassis cluster takes place only on that node and is not propagated to the other nodes in the cluster. Downloads on different nodes are completely independent of each other. In the event of a failover, a download continues only if the server remains reachable from the node from which the command was issued. If the server is no longer reachable on that node, the download stops and returns an error.

Related Documentation

- [Installation Type Overview on page 41](#)

Understanding the Console Port

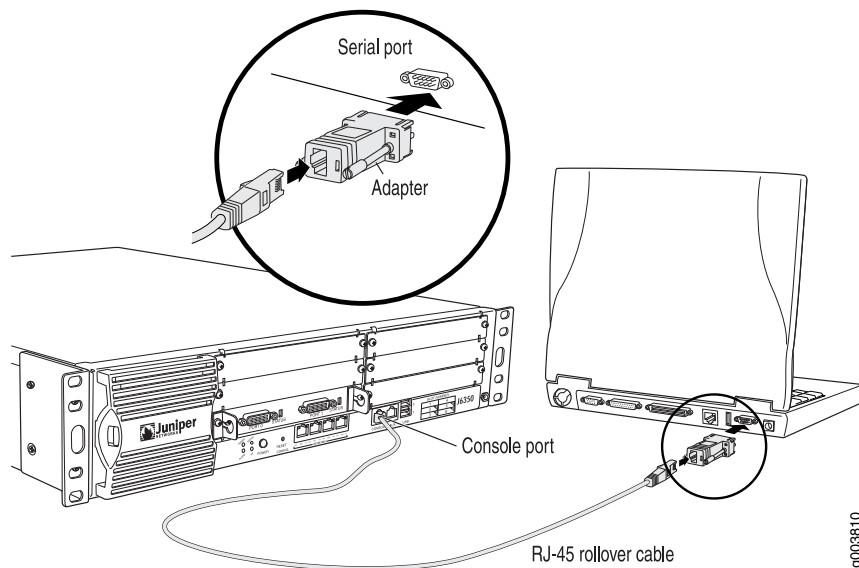
Console ports allow root access to the Junos operating system (Junos OS) devices through a terminal or laptop interface, regardless of the state of the Junos OS device,

unless it is completely powered off. By connecting to the console port, you can access the root level of the Junos OS device without using the network to which the device might or might not be connected. This creates a secondary path to the Junos OS device without relying on the network.

Using the terminal interface provides a technician sitting in a Network Operations Center a long distance away the ability to restore a Junos OS device or perform an initialization configuration securely, using a modem, even if the primary network has failed. Without a connection to the console port, a technician would have to visit the site to perform repairs or initialization. A remote connection to the Junos OS device through a modem requires the cable and connector (provided in the device accessory box), plus a DB-9 male to DB-25 male (or similar) adapter for your modem, which you must purchase separately. For more information about connecting to the console port, see the administration guide for your particular router or switch.

To configure the device initially, you must connect a terminal or laptop computer to the device through the console port, as shown in [Figure 6](#).

Figure 6: Connecting to the Console Port on a Junos OS Device



Related Documentation

- *Accessing a Junos OS Device the First Time*

Backing Up the Existing Installation on Routers

The installation process removes some files stored on the router. In the case of Junos OS, all stored files except the **juniper.conf** and SSH files are removed. Therefore, you must back up your existing installation in case you need to return to it. This topic describes how to back up the existing Junos OS installation on routers.

As of Junos OS Release 15.1, certain platforms run Junos OS based on an upgraded FreeBSD kernel (Junos OS with upgraded FreeBSD). For information about backing up Junos OS with upgraded FreeBSD, see [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#). For the platforms using Junos OS with upgraded FreeBSD, see [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).

For information about backing up the existing installation on SRX Series Services Gateways, see [“Backing Up the Current Installation on SRX Series Devices” on page 56](#).

On routers, you should back up the current installation so that you can return to it if needed.

In a dual Routing Engine system, you need to back up both Routing Engines.

To back up files to the router’s hard disk or solid-state drive (SSD):

- Issue the **request system snapshot** CLI operational command.

```
user@host> request system snapshot
```

When the **request system snapshot** command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The **/root** and **/config** file systems are on the router’s CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router’s hard disk or SSD. When the backup is completed, the current and backup software installations are identical.



NOTE: On routers without a CompactFlash card, where the hard disk is the primary boot device, you cannot back up your software installation. On MX104 routers, which do not have a CompactFlash card, you can back up your software installation on an external USB storage media device.

To back up files on an MX104 to a specified external storage media device:

- Issue the **request system snapshot media** CLI operational command. For example:

```
user@host > request system snapshot media usb1
```

On MX104 routers, when you issue the **request system snapshot** operational command to back up the current software installation, the backup is done on the first USB storage media device.

To back up files to the router's NAND flash device on ACX Series routers:

- Issue the **request system snapshot slice alternate** CLI operational command.

```
user@host > request system snapshot slice alternate
```

When this command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig** on the router's NAND flash device.

To back up files from the NAND flash device to a USB storage media device:

- Issue the **request system snapshot** CLI operational command.

```
user@host> request system snapshot
```

When you issue the **request system snapshot** operational command to back up the NAND flash device, the backup is done on the first USB storage media device.

**Related
Documentation**

- [request system snapshot on page 322](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Backing Up the Current Installation on SRX Series Devices on page 56](#)

Backing Up the Current Installation on SRX Series Devices

This topic includes the following sections:

- [Backing Up the Current Installation on High-End SRX Series Devices on page 56](#)
- [Backing Up the Current Installation on Branch SRX Series Devices on page 57](#)

Backing Up the Current Installation on High-End SRX Series Devices

You should back up the current installation so that you can return to the current software installation. The installation process using the installation package (`jinstall*`, for example) removes all stored files on the device except the `juniper.conf` and SSH files. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program.

To back up Junos OS on the SRX Series devices, issue the **request system snapshot** CLI operational command. This command saves the current software installation on the hard disk, external USB storage media device, or solid-state drive (SSD).

When the **request system snapshot** command is issued, the **/root** file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The **/root** and **/config** file systems are on the device's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the device's hard disk or solid-state drive (SSD). When the backup is completed, the current and backup software installations are identical.

To copy the files to the device's hard disk or solid-state drive (SSD), use the following command:


```
user@host> request system snapshot media
```

Backing Up the Current Installation on Branch SRX Series Devices

On SRX Series devices, you can backup the current Junos OS image and configuration files onto a media (such as a USB or CompactFlash) so that you can retrieve it back if something goes wrong.

To back up the currently running and active file system partitions on the device, use the following command:

```
user@host> request system snapshot media
```

Following options are supported:

- **internal**— Copies the snapshot to internal media.
- **usb**— Copies the snapshot to the USB storage device. This is the default option for Branch SRX Series devices.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)

Installing the Software Package on a Router with a Single Routing Engine

To upgrade the router or switch software, follow these steps:

1. Install the new software package using the **request system software add** command:

```
user@host> request system software add /var/tmp/installation-package
```

installation-package is the name of the installation package; for example **jinstall-9.2R1.8-domestic-signed.tgz**

For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at one time:

```
user@host> request system software add set /var/tmp/installation-package
```

installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.



WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want

to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

For more information about the **request system software add** command, see the [CLI Explorer](#).

2. Reboot the device to start the new software using the **request system reboot** command:

```
user@host> request system reboot
Reboot the system? [yes, no] (no) yes
```



NOTE: You must reboot the device to load the new installation of Junos OS on the device.

To abort the installation, do not reboot the device. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The device then reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not route traffic.

3. Log in and issue the **show version** command to verify the version of the software installed.
4. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see [“Downloading Software” on page 48](#).

The **jweb** installation module adds a device management graphical user interface that you can use to view and configure your device. For more information about the **jweb** package, see [“Installation Modules” on page 14](#).

5. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the **request system snapshot** command to back up the new software.

**Related
Documentation**

- [Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64](#)

Installing the Software Package on a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.



WARNING: If graceful Routing Engine switchover (GRES), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI `delete chassis redundancy` command when prompted. If GRES is enabled, it will be removed with the `redundancy` command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the [edit routing-options] hierarchy level to disable it.

To upgrade the router software, perform the following tasks:

1. [Preparing the Router for the Installation on page 59](#)
2. [Installing Software on the Backup Routing Engine on page 59](#)
3. [Installing Software on the Master Routing Engine on page 61](#)
4. [Finalizing the Installation on page 63](#)

Preparing the Router for the Installation

Perform the following steps before installing the software:

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. From the router command line, enter configuration mode:

```
a. user@host#> configure
   Entering configuration mode

   [edit]
   user@host#
```

3. Disable Routing Engine redundancy:

```
[edit]
user@host# delete chassis redundancy
```

4. Save the configuration change on both Routing Engines:

```
[edit]
user@host# commit synchronize
```

5. Exit out of the CLI configuration mode:

```
[edit]
user@host# exit
```

Installing Software on the Backup Routing Engine

After the router has been prepared, you first install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine and then upgrade or downgrade the software version on the other Routing Engine.

1. Log in to the console port on the other Routing Engine (currently the master).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. Install the new software package using the **request system software add** command:

```
user@host> request system software add validate
/var/tmp/jinstall-9.2R1.8-domestic-signed.tgz
```

For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at the same time:

```
user@host> request system software add set /var/tmp/installation-package
```

installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.

Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.



WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

For more information about the **request system software add** command, see the [CLI Explorer](#).

3. Reboot the router to start the new software using the **request system reboot** command:

```
user@host> request system reboot
Reboot the system? [yes, no] (no) yes
```



NOTE: You must reboot the device to load the new installation of Junos OS on the router.

To abort the installation, do not reboot your device. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the device. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not routing traffic.

4. Log in and issue the **show version** command to verify the version of the software installed.
5. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see [“Downloading Software” on page 48](#).

The **jweb** installation module adds a router management graphical user interface that you can use to view and configure your router. For more information about the **jweb** package, see [“Installation Modules” on page 14](#).

Installing Software on the Master Routing Engine

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine and then upgrade or downgrade the master Routing Engine software:

1. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your router.

2. Transfer routing control to the backup Routing Engine:

```
user@host> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

3. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state           Backup
  Election priority       Master (default)
Routing Engine status:
Slot 1:
  Current state           Master
  Election priority       Backup (default)
```

4. Install the new software package using the **request system software add** command:

```
user@host> request system software add validate
/var/tmp/jinstall-9.2R1.8-domestic-signed.tgz
```

For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can use the **request system software add set** command to install multiple software packages at the same time:

```
user@host> request system software add set /var/tmp/installation-package
```

installation-package can either be a list of installation packages, each separated by a blank space, or the full URL to the directory or tar file containing the list of installation packages.

Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.



WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

For more information about the **request system software add** command, see the [CLI Explorer](#).

5. Reboot the Routing Engine using the **request system reboot** command:

```
user@host> request system reboot
Reboot the system? [yes, no] (no) yes
```



NOTE: You must reboot to load the new installation of Junos OS on the router.

To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall** command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not route traffic.

6. Log in and issue the **show version** command to verify the version of the software installed.
7. (Optional) Add the **jweb** package using the **request system software add** command. Before you can add this package, you must first download the software as you did the installation package. For more information about downloading the **jweb** package, see [“Downloading Software” on page 48](#).

The **jweb** installation module adds a router management graphical user interface that you can use to view and configure your router. For more information about the **jweb** package, see [“Installation Modules” on page 14](#).

8. Transfer routing control back to the master Routing Engine:

```
user@host> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the [CLI Explorer](#).

9. Verify the master Routing Engine (slot 0) is indeed the master Routing Engine:

```

user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state           Master
    Election priority       Master (default)
Routing Engine status:
  Slot 1:
    Current state           Backup
    Election priority       Backup (default)

```

Finalizing the Installation

Once the software is installed on both Routing Engines, you return the router back to its original configuration and back up the new installation.

1. Restore the configuration that existed before you deleted it at the start of this procedure:

```

{backup}
user@host-re0> configure
[edit]
user@host-re0# rollback 1

```

2. Save the configuration change on both Routing Engines:

```

[edit]
user@host-re0> commit synchronize and-quit

```

3. After you have installed the new software and are satisfied that it is successfully running, issue the **request system snapshot** command to back up the new software on both master and backup Routing Engines:

```

{master}
user@host-re0> request system snapshot
{master}
user@host-re0> request routing-engine login other routing-engine
{backup}
user@host-re1> request system snapshot
{backup}

```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

For more information about the **request routing-engine login** command, see the [CLI Explorer](#).



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running copy and backup copy of the software are identical.

Related Documentation • [Repartitioning Routing Engine System Storage To Increase the Swap Partition on page 64](#)

Repartitioning Routing Engine System Storage To Increase the Swap Partition

You can increase the size of the swap partition by repartitioning the drive (hard disk or solid-state drive (SSD)) on the Routing Engine. This feature is first available in Junos OS Release 10.4R5, 11.1R3, and 11.2R1; in earlier Junos OS releases, the swap partition is not increased by the methods described here.

This behavior applies only to Routing Engines with more than 2 GB of RAM. The new size of the swap partition depends on the size of the drive and the amount of Routing Engine RAM.

- When the drive is 32 GB or less, the swap partition is limited to 8 GB.
- When the drive is larger than 32 GB, the swap partition matches the size of the Routing Engine RAM.

To repartition the drive, perform one of the following actions:

- During the installation of a Junos OS software package (**jinstall***), issue the **request system reboot media disk** command to boot from the drive instead of issuing the **request system reboot** command. The drive is automatically repartitioned. The **request system reboot media disk** command repartitions the drive only during a software upgrade.
- Manually partition the drive by issuing the **request system partition hard-disk** command, and then reboot the router when the command completes.



CAUTION: Repartitioning the drive re-creates the `/config` and `/var` directories in the router file system. Although the contents of `/config` and `/var/db` are preserved, the remaining contents of `/var` are lost. For this reason, we recommend that you back up the `/var` directory before you repartition the SSD on a router with this configuration.

Related Documentation

- [Installing the Software Package on a Router with a Single Routing Engine on page 57](#)
- [Installing the Software Package on a Router with Redundant Routing Engines on page 58](#)

Installing Software on EX Series Switches (J-Web Procedure)

You can upgrade software packages on a single fixed-configuration switch, on an individual member of a Virtual Chassis, or for all members of a Virtual Chassis.

You can use the J-Web interface to install software upgrades from a server using FTP or HTTP, or by copying the file to the EX Series switch.

This topic describes:

1. [Installing Software Upgrades from a Server on page 65](#)
2. [Installing Software Upgrades by Uploading Files on page 65](#)

Installing Software Upgrades from a Server

To install software upgrades from a remote server by using FTP or HTTP:

1. Download the software package as described in “[Downloading Software Packages from Juniper Networks](#)” on page 51.
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. In the J-Web interface, select **Maintain > Software > Install Package**.
4. On the Install Remote page, enter information into the fields described in [Table 10](#).
5. Click **Fetch and Install Package**. The software is activated after the switch has rebooted.

Table 10: Install Remote Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	<p>NOTE: The Reboot check box will be disabled if you enter a J-Web Application package name in the Package Location text box. To enable the Reboot check box, enter a Junos package name in the Package Location text box.</p> <p>If this box is checked, the switching platform will automatically reboot when the upgrade is complete.</p>	Check the box if you want the switching platform to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

To install software upgrades by uploading files:

1. Download the software package.
2. In the J-Web interface, select **Maintain>Software>Upload Package**.

3. On the Upload Package page, enter information into the fields described in [Table 11](#).
4. Click **Upload and Install Package**. The software is activated after the switching platform completes the installation procedure.

Table 11: Upload Package Summary

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package.	Type the location of the software package, or click Browse to navigate to the location.
Reboot If Required	Specifies that the switching platform is automatically rebooted when the upgrade is complete.	Select the check box if you want the switching platform to reboot automatically when the upgrade is complete.

- Related Documentation**
- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
 - [Understanding Software Installation on EX Series Switches on page 44](#)
 - [Troubleshooting Software Installation on page 265](#)

Registering the EX Series Switch with the J-Web Interface



NOTE: This topic applies only to the J-Web Application package.

You can register your EX Series switch with the J-Web interface so that you can request technical assistance as and when required. To register an EX Series switch:

1. In the J-Web interface, select **Maintain > Customer Support > Product Registration**. For an EX8200 Virtual Chassis configuration, select the member from the list.
Note the serial number that is displayed.
2. Click **Register**. Enter the serial number in the page that is displayed.

- Related Documentation**
- [EX Series Switch Software Features Overview](#)

Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices

This feature simplifies the upgrading of Junos OS images in cases where there is no console access to an SRX Series device located at a remote site. This functionality allows you to upgrade the Junos OS image with minimum configuration effort by simply copying the image onto a USB flash drive, inserting it into the USB port of the SRX Series device, and performing a few simple steps. You can also use this feature to reformat a boot device and recover an SRX Series device after boot media corruption.

All USB flash drives used on SRX Series devices must have the following features:

- USB 2.0 or later.
- Formatted with a FAT/FAT 32 or MS-DOS file system



NOTE: The Junos OS package on a USB device is commonly stored in the root drive as the only file; for example, `junos-srxsme-15.1X49-D30.3-domestic.tgz`.



CAUTION: Any USB memory product not listed as supported for SRX Series devices has not been tested by Juniper Networks. The use of any unsupported USB memory product could expose your SRX Series device to unpredictable behavior. Juniper Networks Technical Assistance Center (JTAC) can provide only limited support for issues related to unsupported hardware. We strongly recommend that you use only supported USB flash drives.



NOTE: This feature is not supported on chassis clusters.

Before you begin:

- Copy the Junos OS upgrade image and its `autoinstall.conf` file to the USB device.
- Ensure that adequate space is available on the SRX Series device to install the software image.

To prepare the USB flash drive and copy the Junos OS image onto the USB flash drive:

1. Insert the USB flash drive into the USB port of a PC or laptop computer running Windows.
2. From My Computer, right-click the drive Devices with Removable Storage.
3. Format the drive with the FAT/FAT32 file system.
4. Copy the Junos OS image onto the USB device.

For the installation process to succeed, copy only one image onto the USB device. Only images named `junos-srxsme*` are recognized by the system.

5. Check the drive name detected in My Computer for the USB device. Open the command prompt window and type:

```
echo " " > <drive-name>:\autoinstall.conf
```

For example, if the drive detected is drive F, type `echo " " > F:\autoinstall.conf` at the command prompt. This empty file indicates to the system that the automatic installation of the Junos OS image from the USB device is supported.

6. (Optional) Create a text file named `junos-config.conf` and copy the file to the USB device. For example, the following file supports an automatic configuration update during the installation process:

```
system {
  host-name host-1;
  domain-name example.net;
  domain-search [ abc.exmaple.net example.net device1.example.net];
  root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
  }
}
...
routing-options {
  static {
    route 0.0.0.0/0 next-hop 10.207.31.254;
  }
}
```



NOTE: The `junos-config.conf` file is optional, and it is not necessary for the automatic installation of the Junos OS image from the USB device. You can use the `junos-config.conf` file for a backup configuration for recovery or if the existing configuration is accidentally deleted.

**Related
Documentation**

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Installing Junos OS on SRX Series Devices Using a USB Flash Drive

To install the Junos OS image on an SRX Series device using a USB flash drive:

1. Insert the USB flash drive into the USB port of the SRX Series device and wait for the LEDs to blink amber indicating that the SRX Series device detects the Junos OS image.

If the LEDs do not change to amber, press the Power button or turn the device off and then on again and wait for the LEDs to blink amber.

2. Press the **Reset Config** button on the SRX Series device to start the installation and wait for the LEDs to glow steadily amber.

When the LEDs glow green, the Junos OS upgrade image has been successfully installed.

If the USB device is plugged in, the **Reset Config** button always performs as an image upgrade button. Any other functionality of this button is overridden until you remove the USB flash drive.

3. Remove the USB flash drive.

The SRX Series device restarts automatically and loads the new Junos OS version.



NOTE: If an installation error occurs, the LEDs turn red, which might indicate that the Junos OS image on the USB flash drive is corrupted. An installation error can also occur if the current configuration on the SRX Series device is not compatible with the new Junos OS version on the USB or if there is not enough space on the SRX Series device to install the image. You must have console access to the SRX Series device to troubleshoot an installation error.



NOTE: You can use the `set system autoinstallation usb disable` command to prevent the automatic installation from the USB device. After using this command, if you insert the USB device into the USB port of the SRX Series device, the installation process does not work.

Upgrading the Boot Loader on SRX Series Devices

To upgrade the boot loader to the latest version:

1. Upgrade to Junos OS Release 10.0 or later (with or without dual-root support enabled).

The Junos OS 10.0 image contains the latest boot loader binaries in this path:
/boot/uboot, /boot/loader.

2. Enter the shell prompt using the **start shell** command.
3. Run the following command from the shell prompt:

```
bootupgrade -u /boot/uboot -l /boot/loader
```



NOTE: For the new version to take effect, you should reboot the system after upgrading the boot loader.

To verify the boot loader version on the SRX Series device, enter the **show chassis routing-engine bios** command.

```
user@host> show chassis routing-engine bios  
Routing Engine BIOS Version: 1.5
```

The command output displays the boot loader version.



NOTE: You can use the following commands to upgrade U-Boot or perform cyclic redundancy check (CRC):

- `bootupgrade -s -u` – To upgrade the secondary boot loader.
- `bootupgrade -c u-boot` – To check CRC of the boot loader.
- `bootupgrade -s -c u-boot` – To check CRC for the secondary boot loader.
- `bootupgrade -c loader` – To check CRC for the loader on boot loader.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server

You can install Junos OS using the Trivial File Transfer Protocol (TFTP) method. The device is shipped with Junos OS loaded on the primary boot device. During Junos OS installation from the loader, the device retrieves the Junos OS package from a TFTP server. The internal media is then formatted, and the Junos OS image is installed.

From the loader installation, you can:

- Install Junos OS on the device for the first time.
- Recover the system from a file system corruption.



NOTE: Installation from a TFTP server can only be performed using the first onboard Ethernet interface.

Installation from the loader-over-TFTP method does not work reliably over slow speeds or large latency networks.

Before you begin, verify that:

- You have access to the TFTP server with the Junos OS package to be installed.
- That the TFTP server supports BOOTP or DHCP. If the TFTP server does not support BOOTP or DHCP, you must set the environment variables before performing the installation from the TFTP server.
- Functional network connectivity exists between the device and the TFTP server over the first onboard Ethernet interface.

To install the Junos OS image on the internal media of the device:

1. To access the U-boot prompt, use the console connection to connect to the device.
2. Reboot the device.

The following messages appear:

Clearing DRAM..... done BIST check passed. Net: pic init done (err = 0)octeth0 POST Passed

After this message appears, you see the following prompt:

Press SPACE to abort autoboot in 3 seconds

3. Press the space bar to stop the autoboot process.

The => U-boot prompt appears.

4. From the U-boot prompt, configure the environment variables listed in [Table 12](#).

Table 12: Environment Variables Settings

Environment Variables	Description
gatewayip	IP address of the gateway device
ipaddr	IP address of the SRX Series device
netmask	network mask
serverip	IP address of the TFTP server

This example shows you how to configure the environment variables:

```

Clearing DRAM..... done
BIST check passed.
Net: pic init done (err = 0)octeth0
POST Passed
Press SPACE to abort autoboot in 3 seconds
=>
=> setenv ipaddr 10.157.70.170
=> setenv netmask 255.255.255.0
=> setenv gatewayip 10.157.64.1
=> setenv serverip 10.157.60.1
=> saveenv

```

5. Reboot the system using the **reset** command.
6. To access the loader prompt, enter use the console connection to connect to the device.
7. Reboot the device.

The following message appears:

Loading /boot/defaults/loader.conf

After this message appears, you see the following prompt:

Hit [Enter] to boot immediately, or space bar for command prompt.

8. Press the space bar to access the loader prompt.

The **loader>** prompt appears. Enter:

```
loader> install tftp://10.77.25.12/junos-srxsme-10.0R2-domestic.tgz
```



NOTE: The URL path is relative to the TFTP server's TFTP root directory, where the URL is *tftp://tftp-server-ipaddress/package*.

When this command is executed:

- The Junos OS package is downloaded from the TFTP server.
- The internal media on the system is formatted.
- The Junos OS package is installed on the internal media.

After Junos OS is installed, the device boots from the internal media. Once the system boots up with Junos OS Release 10.0 or later, you should upgrade the U-boot and boot loader immediately.



CAUTION: When you install Junos OS using the loader-over-TFTP method, the media is formatted. The process attempts to save the current configuration. We recommend that you back up all important information on the device before using this process.

Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device

To install Junos OS Release 10.0 or later from the boot loader using a USB storage device:

1. Format a USB storage device in MS-DOS format.
2. Copy the Junos OS image onto the USB storage device.
3. Plug the USB storage device into the SRX Series device.
4. Stop the device at the loader prompt and issue the following command:

```
loader> install file:///<image-path-on-usb>
```

An example of a command is as follows:

```
loader> install file:///junos-srxsme-10.0R2-domestic.tgz
```

This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.

5. Once the system boots up with Junos OS Release 10.0 or later, upgrade the U-boot and boot loader immediately.
6. Remove the USB flash drive.

CHAPTER 5

Configuring Zero Touch Provisioning

- [Understanding Zero Touch Provisioning on page 73](#)
- [Configuring Zero Touch Provisioning on page 76](#)

Understanding Zero Touch Provisioning



NOTE: To see which platforms support Zero Touch Provisioning, in a browser, go to [Feature Explorer](#). In the Explore Features section of the Feature Explorer page, select All Features. In the Features Grouped by Feature Family box, select Zero Touch Provisioning. You can also type the name of the feature in the Search for Features edit box. In previous Junos OS releases on EX Series switches, Zero Touch Provisioning was called EZ Touchless Provisioning.

Zero Touch Provisioning allows you to provision new Juniper Networks switches in your network automatically, without manual intervention. When you physically connect a switch to the network and boot it with a default factory configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network. To make sure you have the default factory configuration loaded on the switch, issue the **request system zeroize** command on the switch you want to provision.

The switch uses information that you configure on a Dynamic Host Configuration Protocol (DHCP) server to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default factory configuration.

The Zero Touch Provisioning process will either upgrade or downgrade the Junos OS version. During an downgrade:

- On an EX Series switch, if you downgrade to a software version earlier than Junos OS Release 12.2, in which Zero Touch Provisioning is not supported, the configuration file autoinstall phase of the Zero Touch Provisioning process does not happen.
- On an EX Series switch, to downgrade to a software version that does not support resilient dual-root partitions (Junos OS Release 10.4R2 or earlier), you must perform some manual work on the switch. For more information, see [“Understanding Resilient Dual-Root Partitions on Switches” on page 95](#).



NOTE: On QFX3500 and QFX3600 switches running the original CLI, you cannot use ZTP to upgrade from Junos OS Release 12.2 or later to Junos OS Release 13.2X51-D15 or later.

When you boot a switch with the default factory configuration, the following process happens:

1. If DHCP option 43, suboption 00 (the name of the software image file on the FTP, HTTP, or TFTP server) is configured, the switch compares the version of the provided software image to the version of the software installed on the switch.



NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

2. If DHCP option 43, suboption 02 (a symbolic link to the software image file on the FTP, HTTP, or TFTP server), the switch compares the version of the provided software image to the version of the software installed on the switch.
 - If the Junos OS versions are different, the switch downloads the software image from the FTP, HTTP, or TFTP server, installs the Junos OS, and reboots using the default factory configuration.
 - If the software versions are the same, the switch does not upgrade the software.

3. If DHCP option 43, suboption 01 (the name of the configuration file on the FTP, TFTP, or HTTP server is configured, the switch compares the version of the provided configuration file to the version of the configuration file on the switch.

If DHCP option 43 suboption 01 is not specified, the switch uses the default factory configuration.

If the configuration file version on the FTP, HTTP, or TFTP server is newer than the configuration file on the switch, the configuration file is updated on the switch.

If both DHCP option 43 suboption 01 and suboption 2 are specified, suboption 01 is processed before suboption 02. The Junos OS is upgraded, and then the configuration file is applied.

4. If DHCP option 43, suboption 03 (the transfer mode setting) is configured, the switch accesses the FTP, HTTP, or TFTP server using the specified transfer mode setting—for example, FTP.

If DHCP option 43, suboption 03, is not configured, TFTP becomes the transfer mode automatically.

5. If DHCP option 43, suboption 04 (the name of the software image file on the FTP, HTTP, or TFTP server) is configured, the switch compares the version of the provided software image to the version of the software installed on the switch.



NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

6. If DHCP option 150 or option 66 is specified, the IP address of the FTP, HTTP, or TFTP server is configured.



NOTE: You must configure either option 150 or option 66. If you configure both option 150 and option 66, option 150 takes precedence, and option 66 is ignored. Also, make sure you specify an IP address, not a hostname, because name resolution is not supported.

7. (Optional) If DHCP option 7 is specified, you can configure one or more syslog servers.
8. (Optional) If DHCP option 42 is specified, you can configure one or more NTP servers.
9. (Optional) If DHCP option 12 is specified, you can configure the hostname of the switch.

**Related
Documentation**

- [Configuring Zero Touch Provisioning on page 76](#)

Configuring Zero Touch Provisioning



NOTE: To see which platforms support Zero Touch Provisioning, in a browser, go to [Feature Explorer](#). In the Explore Features section of the Feature Explorer page, select All Features. In the Features Grouped by Feature Family box, select Zero Touch Provisioning. You can also type the name of the feature in the Search for Features edit box. In previous Junos OS releases on EX Series switches, Zero Touch Provisioning was called EZ Touchless Provisioning. Search for that feature name if you want to know if this feature is supported on EX Series switches.

Zero Touch Provisioning allows you to provision new switches in your network automatically, without manual intervention. When you physically connect a switch to the network and boot it with a default configuration, it attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network.

The switch uses information that you configure on a Dynamic Host Control Protocol (DHCP) server to determine whether to perform these actions and to locate the necessary software image and configuration files on the network. If you do not configure the DHCP server to provide this information, the switch boots with the preinstalled software and default configuration.



NOTE: If you have both DHCP and ZTP enabled, the switch broadcasts a DHCP DISCOVER packet every six minutes. If a DHCP server on the network responds with a DHCP ACK packet with DHCP vendor options set with the necessary values to initiate ZTP, then ZTP proceeds.

To disable broadcasting the DHCP DISCOVER packet every six minutes, without performing the ZTP process, manually delete the `auto-image-upgrade` statement located in the `[edit chassis]` hierarchy. If ZTP completes without errors, the `auto-image-upgrade` statement is automatically deleted.



NOTE: For detailed information regarding the DHCP and DHCP options, refer to RFC2131 (<http://www.ietf.org/rfc/rfc2131.txt>) and RFC2132 (www.ietf.org/rfc/rfc2132.txt). Also, this document refers to Internet Systems Consortium (ISC) DHCP version 4.2. For more information regarding this version, refer to <http://www.isc.org/software/dhcp/documentation>.

Before you begin:

- Ensure that the switch has access to the following network resources:

- The DHCP server provides the location of the software image and configuration files on the network

Refer to your DHCP server documentation for configuration instructions.

- The File Transfer Protocol (anonymous FTP), Hypertext Transfer Protocol (HTTP), Trivial File Transfer Protocol (TFTP) server on which the software image and configuration files are stored



NOTE: Although TFTP is supported, we recommend that you use FTP or HTTP instead, because these transport protocols are more reliable.

- A Domain Name System (DNS) server to perform reverse DNS lookup
- (Optional) An NTP server to perform time synchronization on the network
- (Optional) A system log (syslog) server to manage system log messages and alerts
- Locate and record the MAC address printed on the switch chassis.



CAUTION: You cannot commit a configuration while the switch is performing the software update process. If you commit a configuration while the switch is performing the configuration file autoinstallation process, the process stops, and the configuration file is not downloaded from the network.

To configure Zero Touch Provisioning for a switch:

1. Make sure the switch has the default factory configuration installed.
Issue the **request system zeroize** command on the switch that you want to provision.
2. Download the software image file and the configuration file to the FTP, HTTP, TFTP, server that the switch will download these files from.
You can download either one or both of these files.
3. Configure the DHCP server to provide the necessary information to the switch.
Configure IP address assignment.
You can configure dynamic or static IP address assignment for the switch's management address. To determine the switch's management MAC address for static IP address mapping, add 1 to the last byte of the switch's MAC address, which you noted before you began this procedure.
4. Define the format of the vendor-specific information for DHCP option 43 in the dhcpd.conf file.

Here is an example of an ISC DHCP 4.2 server dhcpd.conf file:

```
option space NEW_OP;
option NEW_OP.image-file-name code 0 = text;
option NEW_OP.config-file-name code 1 = text;
option NEW_OP.image-file-type code 2 = text;
```

```
option NEW_OP.transfer-mode code 3 = text;
option NEW_OP.alt-image-file-name code 4 = text;
option NEW_OP-encapsulation code 43 = encapsulate NEW_OP;
```

5. Configure the following DHCP option 43 suboptions:

- Suboption 00: The name of the software image file to install



NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP.image-file-name
"/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
```

- Suboption 01: The name of the configuration file to install

```
option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
```

- Suboption 02: The symbolic link to the software image file to install

```
option NEW_OP.image-file-type "symlink";
```



NOTE: If you do not specify suboption 2, the Zero Touch Provisioning process handles the software image as a filename, not a symbolic link.

- Suboption 03: The transfer mode that the switch uses to access the TFTP/FTP/HTTP server

```
option NEW_OP.transfer-mode "ftp";
```



NOTE: If suboption 03 is not configured, TFTP becomes the transfer mode by default.

- Suboption 04: The name of the software image file to install



NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP.alt-image-file-name
"/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
```

6.



NOTE: You must configure either option 150 or option 66. If you configure both option 150 and option 66, option 150 takes precedence, and option 66 is ignored. Also, make sure you specify an IP address, not a hostname, because name resolution is not supported.

Configure DHCP option 150 to specify the IP address of the FTP, HTTP, or TFTP server.

```
option option-150 code 150 "10.100.31.71";
```

7. Configure DHCP option 66 to specify the IP address of the FTP, HTTP, or TFTP server.

```
option tftp-server-name "10.100.31.71";
```

8. (Optional) Configure DHCP option 7 to specify one or more system log (syslog) servers.

```
option log-servers 10.100.31.72;
```

9. (Optional) Configure DHCP option 42 to specify one or more NTP servers.

```
option ntp-servers 10.100.31.73;
```

10. (Optional) Configure DHCP option 12 to specify the hostname of the switch.

```
option hostname "jn-switch35";
```

The following sample configuration shows the DHCP options you just configured:

```
host jn-switch35 {
  hardware ethernet ac:4b:c8:29:5d:02;
  fixed-address 10.100.31.36;
  option tftp-server-name "10.100.31.71";
  option host-name "jn-switch35";
  option log-servers 10.100.31.72;
  option ntp-servers 10.100.31.73;
  option NEW_OP.image-file-name
    "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
  option NEW_OP.transfer-mode "ftp";
  option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
}
```

Based on the DHCP options you just configured, the following statements are appended to the Junos OS configuration file (for example, `jn-switch35.config`):

```
system {
  host-name jn-switch35;
  syslog {
    host 10.100.31.72 {
      any any;
    }
  }
  ntp {
    server 10.100.31.73;
  }
}
```

11. Connect the switch to the network that includes the DHCP server and the FTP, HTTP, or TFTP server.
12. Boot the switch with the default configuration.
13. Monitor the ZTP process by looking at the following log files.



NOTE: When SLAX (live operating system based on Linux) scripts are issued, the `op-script.log` and `event-script.log` files are produced.

- /var/log/dhcp_logfile
- /var/log/image_load_log
- /var/log/op-script.log
- /var/log/event-script.log

**Related
Documentation**

- [Understanding Zero Touch Provisioning on page 73](#)
- *Understanding NTP Time Servers*
- *Op Script Overview*
- *Understanding DHCP Services for Switches*
- [Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 185](#)

CHAPTER 6

Configuring Automatic Installation of Configuration Files

- [Autoinstallation Overview on page 81](#)
- [Configuring Autoinstallation on SRX Series Devices on page 84](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)

Autoinstallation Overview

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation. The autoinstallation process begins anytime a device is powered on and cannot locate a valid configuration file in the CompactFlash (CF) card. Typically, a configuration file is unavailable when a device is powered on for the first time, or if the configuration file is deleted from the CF card. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the device.

Autoinstallation takes place automatically when you connect an Ethernet or serial port on a new Juniper Networks device to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over

the network. You can use either the J-Web configuration editor or the CLI configuration editor to configure a device for autoinstallation.

This section contains the following topics:

- [Automatic Installation of Configuration Files on page 82](#)
- [Supported Autoinstallation Interfaces and Protocols on page 82](#)
- [Typical Autoinstallation Process on a New Device on page 83](#)

Automatic Installation of Configuration Files

On SRX Series devices, you can specify a remote server where configuration files are located. If a configuration file cannot be found on the device's CompactFlash card, the device automatically retrieves the configuration file from this remote server. For security purposes, you can encrypt these remote files using the DES cipher, and once they have been retrieved, the device decrypts them for use on the server.

To encrypt the files, we recommend the openssl tool. You can get the open SSL tool at: <http://www.openssl.org/>. To encrypt the file, use the following syntax:

```
% openssl enc -des -k passphrase -in original-file -out encrypted-file
```

- ***passphrase***—Passphrase used to encrypt the configuration file. The passphrase should be the name of the file without the path information or file extension.
- ***original-file***—Unencrypted configuration file.
- ***encrypted-file***—Name of the encrypted configuration file.

For example, if you are encrypting the active configuration file **juniper.conf.gz**, the passphrase is **juniper.conf**. The openssl syntax used to encrypt the file is:

```
% openssl enc -des -k juniper.conf -in juniper.conf.gz -out juniper.conf.gz.enc
```

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a device can take place, the device must acquire an IP address. The protocol or protocols you choose for IP address acquisition determine the device interface to connect to the network for autoinstallation. The device detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface or a serial LAN or WAN interface. [Table 13](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 13: Interfaces and Protocols for IP Address Acquisition During Autoinstallation

Interface and Encapsulation Type	Protocol for Autoinstallation
Ethernet LAN interface with High-Level Data Link Control (HDLC)	DHCP, BOOTP, or Reverse Address Resolution Protocol (RARP)
Serial WAN interface with HDLC	Serial Line Address Resolution Protocol (SLARP)

Table 13: Interfaces and Protocols for IP Address Acquisition During Autoinstallation (*continued*)

Interface and Encapsulation Type	Protocol for Autoinstallation
Serial WAN interface with Frame Relay	BOOTP

If the server with the autoinstallation configuration file is not on the same LAN segment as the new device, or if a specific device is required by the network, you must configure an intermediate device directly attached to the new device through which the new device can send Trivial File Transfer Protocol (TFTP), BOOTP, and Domain Name System (DNS) requests. In this case, you specify the IP address of the intermediate device as the location to receive TFTP requests for autoinstallation.

Typical Autoinstallation Process on a New Device

When a device is powered on for the first time, it performs the following autoinstallation tasks:

1. The new device sends out DHCP, BOOTP, RARP, or SLARP requests on each connected interface simultaneously to obtain an IP address.

If a DHCP server responds, it provides the device with some or all of the following information:

- An IP address and subnet mask for the autoinstallation interface.
- The location of the TFTP (typically), Hypertext Transfer Protocol (HTTP), or FTP server on which the configuration file is stored.
- The name of the configuration file to be requested from the TFTP server.
- The IP address or hostname of the TFTP server.

If the DHCP server provides only the hostname, a DNS server must be available on the network to resolve the name to an IP address.

- The IP address of an intermediate device if the configuration server is on a different LAN segment from the new device.
2. After the new device acquires an IP address, the autoinstallation process on the device attempts to download a configuration file in the following ways:
 - a. If the DHCP server specifies the host-specific configuration file (boot file) **hostname.conf**, the device uses that filename in the TFTP server request. (In the filename, **hostname** is the hostname of the new device.) The autoinstallation process on the new device makes three unicast TFTP requests for **hostname.conf**. If these attempts fail, the device broadcasts three requests to any available TFTP server for the file.
 - b. If the new device cannot locate **hostname.conf**, the autoinstallation process unicasts or broadcasts TFTP requests for a default device configuration file called **network.conf**, which contains hostname-to-IP address mapping information, to attempt to find its hostname.

- c. If **network.conf** contains no hostname entry for the new device, the autoinstallation process sends out a DNS request and attempts to resolve the new device's IP address to a hostname.
 - d. If the new device can determine its hostname, it sends a TFTP request for the **hostname.conf** file.
 - e. If the new device is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file **router.conf**.
3. After the new device locates a configuration file on a TFTP server, autoinstallation downloads the file, installs the file on the device, and commits the configuration.

**NOTE:**

- If you configure the DHCP server to provide only the TFTP server hostname, add an IP address-to-hostname mapping entry for the TFTP server to the DNS database file on the DNS server in the network.
 - If the new device is not on the same network segment as the DHCP server (or other device providing IP address resolution), configure an existing device as an intermediate to receive TFTP and DNS requests and forward them to the TFTP server and the DNS server. You must configure the LAN or serial interface on the intermediate device with the IP addresses of the hosts providing TFTP and DNS service. Connect this interface to the new device.
-

Related Documentation

- [Configuring Autoinstallation on SRX Series Devices on page 84](#)

Configuring Autoinstallation on SRX Series Devices

This example shows how to configure a device for autoinstallation.

- [Requirements on page 84](#)
- [Overview on page 85](#)
- [Configuration on page 85](#)
- [Verification on page 86](#)

Requirements

Before you begin:

- Configure a DHCP server on your network to meet your network requirements. You can configure a device to operate as a DHCP server.
- Create one of the following configuration files, and store it on a TFTP server in the network (see ["Configuration Files" on page 15](#)):

- A host-specific file with the name **hostname.conf** for each device undergoing autoinstallation. Replace **hostname** with the name of a device. The **hostname.conf** file typically contains all the configuration information necessary for the device with this hostname.
- A default configuration file named **router.conf** with the minimum configuration necessary to enable you to telnet into the new device for further configuration.
- Physically attach the device to the network using one or more of the following interface types:
 - Fast Ethernet
 - Gigabit Ethernet
 - Serial with HDLC encapsulation

Overview

No configuration is required on a device on which you are performing autoinstallation, because it is an automated process. However, to simplify the process, you can specify one or more interfaces, protocols, and configuration servers to be used for autoinstallation.

The device uses these protocols to send a request for an IP address for the interface.

- BOOTP—Sends requests over all interfaces.
- RARP—Sends requests over Ethernet interfaces.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system autoinstallation configuration-servers tftp://tftpconfig.sp.com
set system autoinstallation interfaces ge-0/0/0 bootp rarp
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To configure a device for autoinstallation:

1. Enable autoinstallation and specify the URL address of one or more servers from which to obtain configuration files.

```
[edit system]
user@host# set autoinstallation configuration-servers tftp://tftpconfig.sp.com
```



NOTE: You can also use an FTP address, for example, `ftp://user:password@sftpconfig.sp.com`.

2. Configure one or more Ethernet or serial interfaces to perform autoinstallation, and configure one or two procurement protocols for each interface.

[edit system]

user@host# **set autoinstallation interfaces ge-0/0/0 bootp rarp**

Results From configuration mode, confirm your configuration by entering the **show system autoinstallation status** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]

user@host# **show system autoinstallation status**

```
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  State: Configuration Acquisition
  Acquired:
    Address: 192.168.124.75
    Hostname: host-ge-000
    Hostname source: DNS
    Configuration filename: router-ge-000.conf
    Configuration filename server: 10.25.100.3
  Address acquisition:
    Protocol: BOOTP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: When there is a user-specified configuration for a particular interface, the factory default for that interface should be deleted. Having two configurations for the same device might lead to errors. For example, if PPP encapsulation is set on a T1 interface through user configuration while the factory default configuration configures CISCO HLDC on the same interface, then the interface might not come up and the following error will be logged in the message file: “DCD_CONFIG_WRITE_FAILED failed.”

Verification

Confirm that the configuration is working properly.

- [Verifying Autoinstallation on page 86](#)

Verifying Autoinstallation

Purpose Verify that the device has been configured for autoinstallation.

Action From operational mode, enter the **show system autoinstallation status** command. The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the device when it is deployed on the network.

Related Documentation

- [Autoinstallation Overview on page 81](#)

Configuring Autoinstallation on JNU Satellite Devices

No configuration is required on a device on which you are performing autoinstallation because it is an automated process. However, to simplify the process, you can specify one or more interfaces, protocols, and configuration servers to be used for autoinstallation. In this scenario, satellite devices, such as EX Series Ethernet Switches, QFX Series devices, and ACX Series Universal Access Routers, that are managed by the controller are considered.

To configure autoinstallation:

1. Load the JNU factory-default configuration file on the satellite device to enable the device to function in JNU mode.

```
user@satellite# load override /etc/config/jnu-factory.conf
```

An override operation discards the current candidate configuration and loads the configuration in the specified filename or the one that you type at the terminal. When you use the override option and commit the configuration, all system processes reparse the configuration.

2. Specify the URL address of one or more servers from which to obtain configuration files.

```
[edit system]
```

```
user@host# set autoinstallation configuration-servers tftp://tftpconfig.sp.com
```



NOTE: You can also use an HTTP or FTP address—for example, `http://user:password@httpconfig.sp.com` or `ftp://user:password@sftpconfig.sp.com`.

3. Configure one or more Ethernet interfaces to perform autoinstallation and IP address acquisition protocols for each interface. The router uses the protocols to send a request for an IP address for the interface:

```
[edit system]
```

```
user@host# set autoinstallation interfaces ge-0/0/0 bootp
```

4. Set the root password, entering a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string.

Choose one of the following:

- To enter a clear-text password, use the following command:

```
[edit system]
```

```
user@host# set root-authentication plain-text-password
```

```
New password: type password here
```

```
Retype new password: retype password here
```

- To enter a password that is already encrypted, use the following command:

```
[edit]
```

```
root# set system root-authentication encrypted-password encrypted-password
```

- To enter an SSH public key, use the following command:

```
[edit]
```

```
root# set system root-authentication ssh-rsa key
```

5. Save the Junos OS configuration changes, activate the configuration on the device and exit configuration mode, using the **commit-and-quit** command.

```
[edit]
```

```
user@host# commit-and-quit
```

When the satellite device reboots, it triggers the autoinstallation mechanism to retrieve its initial configuration and downloads the settings from the configuration file stored on a configuration server in the network. On the controller, you must enable the FTP service by using the **set system services ftp** command and save the configuration on the satellite device at the **/var/jnu/** directory.

The following configuration is generated on the satellite device as a result of the preceding procedure to configure autoinstallation:

```
system {
  autoinstallation {
    traceoptions {
      flags {
        all;
      }
      file autod;
      level all;
    }
    delete-after-commit; /* After initial config, no need to keep */
    interfaces {
      ge-* {
        bootp;
      }
      xe-* {
        bootp;
      }
      configuration-servers {
        "ftp://192.168.0.1/var/jnu/sat1.conf";
      }
    }
  }
  root-authentication {
    encrypted-password "$ABC123";
  }
}
```


- Related Documentation**
- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
 - [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
 - [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
 - [autoinstallation on page 280](#)
 - [delete-after-commit \(JNU Satellites\) on page 284](#)
 - [configuration-servers](#)

Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group

Autoinstallation provides automatic configuration for a new router that you connect to the network and power on, or for a router configured for autoinstallation. The autoinstallation process begins anytime a router is powered on and cannot locate a valid configuration file in the CompactFlash card. Typically, a configuration file is unavailable when a router is powered on for the first time, or if the configuration file is deleted from the CompactFlash card. The autoinstallation feature enables you to deploy multiple routers from a central location in the network.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the router.

Autoinstallation takes place automatically when you connect an Ethernet interface on a new Juniper Networks router to the network and power on the router. To simplify the process, you can explicitly enable autoinstallation on a router and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

This topic describes:

- [Supported Autoinstallation Interfaces and Protocols on page 89](#)
- [Typical Autoinstallation Process on a New Router on page 90](#)

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a router can take place, the router must acquire an IP address or a USB key. The protocol or protocols you choose for IP address acquisition determine the router interface to connect to the network for autoinstallation. The router detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface. For IP address acquisition, the JNU satellite router uses DHCP, BOOTP, or Reverse Address Resolution Protocol (RARP) on an Ethernet LAN interface.

If the server with the autoinstallation configuration file is not on the same LAN segment as the new router, or if a specific router is required by the network, you must configure an intermediate router directly attached to the new router, through which the new router can send HTTP, FTP, Trivial File Transfer Protocol (TFTP), BOOTP, and Domain Name

System (DNS) requests. In this case, you specify the IP address of the intermediate router as the location to receive HTTP, FTP, or TFTP requests for autoinstallation.

Typical Autoinstallation Process on a New Router

When a router is powered on for the first time, it performs the following autoinstallation tasks:

1. The new router sends out DHCP, BOOTP, or RARP requests on each connected interface simultaneously to obtain an IP address.

If a DHCP server responds, it provides the router with some or all of the following information:

- An IP address and subnet mask for the autoinstallation interface.
- The location of the TFTP (typically), Hypertext Transfer Protocol (HTTP), or FTP server on which the configuration file is stored.
- The name of the configuration file to be requested from the HTTP, FTP, or TFTP server.
- The IP address or hostname of the HTTP, FTP, or TFTP server.

If the DHCP server provides only the hostname, a DNS server must be available on the network to resolve the name to an IP address.

- The IP address of an intermediate router if the configuration server is on a different LAN segment from the new router.
2. After the new router acquires an IP address, the autoinstallation process on the router attempts to download a configuration file in the following ways:
 - a. If the configuration file is specified as a URL, the router fetches the configuration file from the URL by using HTTP, FTP, or TFTP depending on the protocol specified in the URL.
 - b. If the DHCP server specifies the host-specific configuration file (boot file) **hostname.conf**, the router uses that filename in the TFTP server request. (In the filename, **hostname** is the hostname of the new router.) The autoinstallation process on the new router makes three unicast TFTP requests for **hostname.conf**. If these attempts fail, the router broadcasts three requests to any available TFTP server for the file.
 - c. If the new router cannot locate **hostname.conf**, the autoinstallation process unicasts or broadcasts TFTP requests for a default router configuration file called **network.conf**, which contains hostname-to-IP address mapping information, to attempt to find its hostname.
 - d. If **network.conf** contains no hostname entry for the new router, the autoinstallation process sends out a DNS request and attempts to resolve the new router's IP address to a hostname.

- e. If the new router can determine its hostname, it sends a TFTP request for the **hostname.conf** file.
 - f. If the new router is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file **router.conf**.
3. After the new router locates a configuration file on a TFTP server, the autoinstallation process downloads the file, installs the file on the router, and commits the configuration.

Related Documentation

- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
- [autoinstallation on page 280](#)
- [delete-after-commit \(JNU Satellites\) on page 284](#)
- [configuration-servers](#)

Autoinstallation of Satellite Devices in a Junos Node Unifier Group

In a Junos Node Unifier (JNU) group that contains an MX Series router as a controller that manages satellite devices, such as EX Series Ethernet Switches, QFX Series devices, and ACX Series Universal Access Routers, the autoinstallation functionality is supported for the satellite devices. JNU has an autoinstallation mechanism that enables a satellite device to configure itself out-of-the-box with no manual intervention, using the configuration available either on the network or locally through a removable media, or using a combination of both. This autoinstallation method is also called the *zero-touch* facility.

The zero-touch configuration delivers the following benefits:

- The router can be sent from the warehouse to the deployment site without any preconfiguration steps.
- The procedure required to deploy the device at the cell site is simplified, resulting in reduced operational and administrative costs.
- You can roll out large numbers of these devices in a very short time.

The factory default setting is autoinstallation-enabled. After you make the first configuration to the router, you can do either of the following:

- A JNU factory default file, **jnu-factory.conf**, is present in the **/etc/config/** directory and contains the configuration to perform autoinstallation on satellite devices. The zero-touch configuration can be disabled by including the **delete-after-commit** statement at the **[edit system autoinstallation]** hierarchy level and committing the configuration. This way, the saved configuration is used the next time the system reboots.

- Alternatively, if the router must get the configuration from the server each time a system reboot occurs, the zero-touch configuration must not be changed (that is, you must not include the **delete-after-commit** statement at the **[edit system autoinstallation]** hierarchy level and commit the settings).

Related Documentation

- [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [Verifying Autoinstallation on JNU Satellite Devices on page 92](#)
- [autoinstallation on page 280](#)
- [delete-after-commit \(JNU Satellites\) on page 284](#)
- [configuration-servers](#)

Verifying Autoinstallation on JNU Satellite Devices

- Purpose** After you have configured autoinstallation, display the status of autoinstallation on a satellite device, such as an ACX Series router, an EX Series switch, or a QFX Series device, in a Junos Node Unifier (JNU) group that is managed by a controller, which is an MX Series router.
- Action** From the CLI, enter the **show system autoinstallation status** command. The following example displays the autoinstallation settings of an ACX Series router that operates as a satellite in a JNU group.

Sample Output

```
user@host> show system autoinstallation status
Autoinstallation status:
  Master state: Active
  Last committed file: None
  Configuration server of last committed file: 10.25.100.1
  Interface:
    Name: ge-0/1/0
    State: Configuration Acquisition
    Acquired:
      Address: 192.168.124.75
      Hostname: host-ge-000
      Hostname source: DNS
      Configuration filename: router-ge-000.conf
      Configuration filename server: 10.25.100.3
    Address acquisition:
      Protocol: DHCP Client
      Acquired address: None
      Protocol: RARP Client
      Acquired address: None
  Interface:
    Name: ge-0/1/1
    State: None
    Address acquisition:
      Protocol: DHCP Client
      Acquired address: None
      Protocol: RARP Client
```

Acquired address: None

Meaning The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the router when it is deployed on the network.

Related Documentation

- [Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91](#)
- [Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89](#)
- [Configuring Autoinstallation on JNU Satellite Devices on page 87](#)
- [autoinstallation on page 280](#)
- [delete-after-commit \(JNU Satellites\) on page 284](#)
- [configuration-servers](#)
- [show system autoinstallation status on page 383](#)

CHAPTER 7

Configuring Dual-Root Partitions for High Availability

- [Understanding Resilient Dual-Root Partitions on Switches on page 95](#)
- [Resilient Dual-Root Partitions Frequently Asked Questions on page 99](#)
- [Dual-Root Partitioning Scheme on SRX Series Devices on page 105](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110](#)

Understanding Resilient Dual-Root Partitions on Switches

Resilient dual-root partitioning, introduced on Juniper Networks EX Series Ethernet Switches in Juniper Networks Junos operating system (Junos OS) Release 10.4R3, provides additional resiliency to switches in the following ways:

- Allows the switch to boot transparently from the second (alternate) root partition if the system fails to boot from the primary root partition.
- Provides separation of the root Junos OS file system from the `/var` file system. If corruption occurs in the `/var` file system (a higher probability than in the root file system because of the greater frequency of reads and writes in `/var`), the root file system is insulated from the corruption.



NOTE: For instructions on upgrading to a release that supports resilient dual-root partitions from a release that does not, see the release notes. The procedure for upgrading to a resilient dual-root partition release is different from the normal upgrade procedure.

This topic covers:

- [Resilient Dual-Root Partition Scheme \(Junos OS Release 10.4R3 and Later\) on page 96](#)
- [Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature on page 96](#)

- [Earlier Partition Scheme \(Junos OS Release 10.4R2 and Earlier\)](#) on page 97
- [Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases](#) on page 98

Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)

EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with a root partition scheme that is optimized for resiliency, as shown in [Table 14](#).

Table 14: Resilient Dual-Root Partition Scheme

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/	/	/var	/var/tmp	/config
(root Junos OS)	(root Junos OS)			

In the resilient dual-root partition scheme, the **/var** file system is contained in a separate slice (Slice 3) from the root file systems; the **/config** directory is contained in its own slice (Slice 4); and switches ship from the factory with identical Junos OS images in Slice 1 and Slice 2. The **/var** file system, which has a greater frequency of reads and writes than the root file systems and is therefore more likely to have corruption issues, is isolated from the root directories and the **/config** directory. If the switch fails to boot from the active partition, the switch automatically boots from the alternate root partition and triggers an alarm.

Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature

Resilient dual-root partitioning also provides the *automatic snapshot* feature, which allows the switch to automatically fix a corrupt Junos OS file in the primary root partition. If the automatic snapshot feature is enabled, the switch automatically takes a snapshot of the Junos OS root file system in the alternate root partition and copies it onto the primary root partition, thereby repairing the corrupt file in the primary root partition. The automatic snapshot procedure takes place whenever the system reboots from the alternate root partition, regardless of whether the reboot is due to a command or due to corruption of the primary root partition.

**NOTE:**

- EX9200 switches do not support the automatic snapshot feature.
- The automatic snapshot feature is enabled by default on the following EX Series switches:
 - EX4550 switches
 - EX Series switches that ship with Junos OS Release 12.3R1 or later
- The automatic snapshot feature is disabled by default on EX Series switches (except the EX4550 switches) running Junos OS Release 12.2 or earlier.
- If the automatic snapshot feature was disabled by default before the switch was upgraded to Junos OS Release 12.3R1 or later, the feature remains disabled (for backward compatibility) by default after the upgrade.
- If the automatic snapshot feature is enabled in a Virtual Chassis configuration, the automatic snapshot procedure takes place whenever any member of the Virtual Chassis reboots from its alternate root partition.
- You can enable the automatic snapshot feature by configuring the `auto-snapshot` statement at the `[edit system]` hierarchy level.

The automatic snapshot feature provides an additional layer of fault protection if you maintain the same version of Junos OS in both partitions of resilient dual-root partitions. When **auto-snapshot** is enabled, repair happens automatically. Therefore, the switch does not issue an alarm to indicate that the system has rebooted from the alternate partition. However, it does log the event. You cannot execute a manual snapshot when an automatic snapshot procedure is in process. The login banner indicates that an automatic snapshot operation is in progress and that banner is removed only after the snapshot operation is complete. The next reboot happens from the primary partition.



NOTE: EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with identical Junos OS images in the primary root partition (Slice 1) and the alternate root partition (Slice 2).

However, if you do *not* maintain the same version of Junos OS in both partitions, you might want to disable the automatic snapshot feature. If you have an earlier version of Junos OS in the alternate partition and the system reboots from the alternate root partition, the automatic snapshot feature causes the later Junos OS version to be replaced with the earlier version.

When automatic snapshot is disabled and the system reboots from the alternate root partition, it triggers an alarm indicating that the system has rebooted from its alternate partition.

Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)

The partition scheme used in Junos OS 10.4R2 and earlier is shown in [Table 15](#).

Table 15: Earlier Partition Scheme

Slice 1		Slice 2		Slice 3	
s1a	s1f	s2a	s2f	s3d	s3e
/ (root Junos OS)		(empty until initial software upgrade)		/var/tmp	/config

This is the partitioning scheme for a switch shipped with Release 10.4R2 or earlier (or after you reformat the disk during a downgrade from Release 10.4R3 or later to Release 10.4R2 or earlier). In this partitioning scheme, the switch comes from the factory with only one Junos OS image installed in the root Junos OS partition of Slice 1. The first time that you perform a software upgrade, the new Junos OS image is installed in Slice 2. If the switch fails to boot, you must manually trigger it to boot from the alternate partition (rebooting from the alternate partition does not occur automatically).

Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases

Upgrading from Release 10.4R2 or earlier to Release 10.4R3 or later differs from other upgrades in two important ways:

- You must install a new loader software package in addition to installing the new Junos OS image.
- Rebooting after the upgrade reformats the disk from three partitions to four partitions. See [Table 14](#).

You can perform all operations for this special software upgrade from the CLI.



CAUTION: Back up any important log files because the `/var/log` files are not saved or restored during an upgrade from Release 10.4R2 or earlier to a release that supports resilient dual-root partitions (Release 10.4R3 or later).

We recommend that you also save your `/config` files and any important log files to an external medium because if there is a power interruption during the upgrade process, they might be lost.

Related Documentation

- [Resilient Dual-Root Partitions Frequently Asked Questions on page 99](#)

Resilient Dual-Root Partitions Frequently Asked Questions



NOTE: This task uses Junos OS for EX Series switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Resilient Dual-Root Partitions Frequently Asked Questions*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

This FAQ addresses questions regarding resilient dual-root partitions on EX Series switches and upgrading to Junos OS releases that support resilient dual-root partitions. The resilient dual-root partition feature was introduced on EX Series switches at Junos OS Release 10.4R3. It provides additional resiliency for EX Series switches.

This FAQ covers the following questions:

- [How Does Upgrading to Junos OS Release 10.4R3 and Later Differ from Normal Upgrades? on page 99](#)
- [What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time? on page 100](#)
- [Can I Downgrade Junos OS Without Downgrading the Loader Software? on page 101](#)
- [Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI? on page 101](#)
- [Will I Lose My Configuration During an Upgrade? on page 102](#)
- [How Long Will the Upgrade Process Take? on page 102](#)
- [What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Enabled? on page 102](#)
- [What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Not Enabled? on page 103](#)
- [How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System? on page 103](#)
- [Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release? on page 104](#)
- [Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch? on page 104](#)
- [Where Can I Find Instructions for Upgrading? on page 104](#)

How Does Upgrading to Junos OS Release 10.4R3 and Later Differ from Normal Upgrades?

Upgrading from Junos OS Release 10.4R2 or earlier to Release 10.4R3 or later differs from other upgrades in these ways:

- You must upgrade the loader software in addition to installing the new Junos OS image.
- Rebooting after the upgrade reformats the disk from three partitions to four partitions.

- The upgrade process and the reboot take longer time because of the additional time required for upgrading the loader software and for the first reboot after the Junos OS installation (longer than normal because it reformats the disk from three partitions to four). Also, EX8200 switches require an additional reboot per Routing Engine as part of the loader software upgrade.

What Happens If I Do Not Upgrade Both the Loader Software and Junos OS at the Same Time?

You must install a new loader software package if you are upgrading to a release that supports resilient dual-root partitions (Release 10.4R3 and later) from an earlier release (Release 10.4R2 and earlier).

If you upgrade to Release 10.4R3 or later from Release 10.4R2 or earlier and do not upgrade the loader software, the switch will come up and function normally. However, if the switch encounters a problem and cannot boot from the active root partition, it cannot transparently boot from the alternate root partition and you will need to perform a manual reboot.



NOTE: Starting with Junos OS Release 11.4R4, when an EX Series switch boots from the flash memory, and a valid jloader firmware image does not exist or is corrupted in the upgrade bank, the following alarm is displayed: “Upgrade bank is empty or corrupted for FPC 0, please do standard upgrade sequence.” To resolve this issue, contact JTAC for assistance in determining the version of jloader firmware that you need to install.

Table 16: Combinations of Junos OS Versions and Loader Software Versions

Junos OS Release	Loader Software	Notes
Release 10.4R3 and later	<p>New loader software</p> <p>For all EX Series switches except EX8200 switches: U-Boot 1.1.6 (Mar 11 2011 - 04:39:06) 1.0.0 (Contains version 1.0.0 after the timestamp.)</p> <p>For EX8200 switches: U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) 3.5.0 (Contains version 3.5.0.)</p>	Recommended
Release 10.4R2 and earlier	Old loader software	If you downgrade to Release 10.4R2 or earlier after having upgraded to the new loader software version, you do not need to downgrade the loader software. The switch will function normally.

Table 16: Combinations of Junos OS Versions and Loader Software Versions (*continued*)

Junos OS Release	Loader Software	Notes
Release 10.4R3 and later	<p>Old loader software</p> <p>For all EX Series switches except EX8200 switches: U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) (Does not contain a version number after the timestamp)</p> <p>For EX8200 switches: U-Boot 1.1.6 (Jan 11 2008 - 05:24:35) 2.3.0 (Contains a version earlier than 3.5.0.)</p>	The switch will come up and function normally. However, in the event that the switch cannot boot from the active root partition, it will not transparently boot up from the alternate root partition.
Release 10.4R2 and earlier	<p>New loader software</p> <p>NOTE: For EX Series switches except EX8200 switches, in Release 10.4R2 and earlier the version number after the timestamp (shown in the previous row) is not displayed, and you cannot verify whether the old or the new loader software version is installed.</p>	The switch will come up and function normally.

Can I Downgrade Junos OS Without Downgrading the Loader Software?

Yes, when you downgrade from most releases, the new loader software runs seamlessly with the earlier Junos OS version.



NOTE: If you downgrade specifically from Release 10.4R3 or Release 11.1R1 to 10.4R2 or earlier (that is, to a release that does not support resilient dual-root partitions), you must disable the boot-sequencing function. If you do not take this action, the switch will boot on each subsequent reboot from the alternate root partition rather than from the active partition.

Disable the boot-sequencing function in one of two ways:

- From the shell as the root user:

```
% nvram setenv boot.btsq.disable 1
```
- From a console connection, reboot and stop at the u-boot prompt (Ctrl+c):

```
=> setenv boot.btsq.disable 1
=> saveenv
```

If you are downgrading from Release 10.4R4 or from Release 11.1R2 or later to Release 10.4R2 or earlier, you do not need to disable the boot-sequencing function—the software does it automatically.

Can I Upgrade to a Resilient Dual-Root Partition Release by Using the CLI?

Yes, you can perform the entire upgrade to resilient dual-root partitions from the CLI. You download both the new loader software and Junos OS packages and install them

from the CLI. During the final reboot, the disk is automatically reformatted from three to four partitions.

Will I Lose My Configuration During an Upgrade?

Configuration files are preserved and restored during the reformatting of the disk. We recommend that you save your configuration before upgrading because if there is a power interruption during the installation process, the files might be lost.

How Long Will the Upgrade Process Take?

The process of upgrading to a resilient dual-root partition release takes longer than other upgrades because of the additional step of upgrading the loader software and the longer reboot time required while the disk is reformatted to four partitions during the reboot of the switch that completes the Junos OS upgrade. The reformat results in an additional reboot time of 5 to 10 minutes for EX2200, EX3200, EX4200, and EX4500 switches. For EX8200 switches, the reboot time increases by 10 to 25 minutes per Routing Engine, and additional reboots are required.

What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Enabled?

If the automatic snapshot feature is enabled during a reboot, the system automatically takes a snapshot of Junos OS from the alternate root partition (Slice 2) and copies it onto the primary root partition (Slice 1). The system checks each file system partition for corruption. [Table 17](#) shows the action the system takes if corruption is detected and the corrective action that you can take.

Table 17: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/	/	/var	/var/tmp	/config
(root Junos OS)	(root Junos OS)			
If a root directory (/) is corrupted, the corrupted file system is not mounted. The switch automatically takes a snapshot of the Junos OS root file system and copies it onto the primary root partition. It boots from the alternate slice, but the next reboot happens from the primary slice.		During early boot, the integrity of /var, /var/tmp, and /config files is verified. If they are corrupted, the corrupted slice is reformatted and the file directory in that slice is lost.		
Corrective action: No corrective action is required.		Corrective action: Restore the /var or /config files from the external backup.		

What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot Is Not Enabled?

During a reboot, the system checks each file system partition for corruption. [Table 18](#) shows the action the system takes if corruption is detected and the corrective action that you can take.

Table 18: Actions If Corrupt Files Are Found

Slice 1	Slice 2	Slice 3		Slice 4
s1a	s2a	s3e	s3d	s4d
/	/	/var	/var/tmp	/config
(root Junos OS)	(root Junos OS)			
If a root directory (/) is corrupted, the corrupted file system is not mounted and the switch boots from the alternate slice.		During early boot, the integrity of /var, /var/tmp, and /config files is verified. If they are corrupted, the corrupted slice is reformatted and the file directory in that slice is lost.		
Corrective action: Issue a request system snapshot command from the good root directory to the corrupted slice.		Corrective action: Restore the /var or /config files from the external backup.		

How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System?

If the switch detects corruption in the primary root file system, it boots from the alternate root partition. When this occurs, the type of notification depends on whether you have enabled the automatic snapshot feature or not:

- If the automatic snapshot feature is not enabled:
 - If you are logged in through the console port or the management port:


```
WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE
```

It is possible that the primary copy of JUNOS failed to boot up properly, and so this device has booted from the backup copy.

Please re-install JUNOS to recover the primary copy in case it has been corrupted.
 - The following message is displayed when you issue **show chassis alarms**:

```
user@switch> show chassis alarms
1 alarms currently active
Alarm time           Class  Description
2011-02-17 05:48:49 PST  Minor  Host 0 Boot from backup root
```

- If the automatic snapshot feature is enabled:
 - A banner message appears, indicating that an automatic snapshot operation is in progress. The banner message disappears when the snapshot operation is complete.
 - No alarm is issued to indicate that the switch has been rebooted from the alternate partition. However, the switch does log the event.

Can I Use Automatic Software Update and Download to Upgrade to a Resilient Dual-Root Partition Release?

Automatic software update and automatic software download are both supported with upgrading to releases that support resilient dual-root partitions. However, after an automatic installation, you must take the extra step of upgrading the loader software.

Automatic software update is for new members added to a Virtual Chassis that do not have the same software as the master. Once this feature is configured on the Virtual Chassis, any new member added with a different software version will be upgraded automatically.

Automatic software download uses the DHCP message exchange process to download and install software packages.

Why Is the Message "At least one package installed on this device has limited support" Displayed When Users Log In to a Switch?

The following message might be displayed when a user logs in:

```
Logging to master
..Password:
--- JUNOS 10.4R3.4 built 2011-03-19 22:06:32 UTC
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
```

This message can be safely ignored or you can permanently remove it. It appears because the jloader package file has been detected, and it only appears when Junos OS is installed before the loader software is upgraded (required only for EX8200 switches).

You can permanently remove this message by removing the jloader package and rebooting the system:

```
user@switch> request system software delete jloader-ex-zzzz
user@switch> request system reboot
```

Where *jloader-ex-zzzz* represents the name of the jloader software package for your platform—jloader-ex2200 for an EX2200 switch, jloader-ex3242 for an EX3200 or EX4200 switch, or jloader-ex8200 for an EX8200 switch.

Where Can I Find Instructions for Upgrading?

The procedure for upgrading to a release that supports resilient dual-root partitions (from a release that does not) is different from the normal upgrade procedure. For instructions on upgrading to a resilient dual-root partition release, see the Release Notes.

Related Documentation

- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)

- [Troubleshooting Software Installation on page 265](#)
- [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 268](#)
- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)

Dual-Root Partitioning Scheme on SRX Series Devices

Junos OS Release 10.0 and later support dual-root partitioning on SRX Series devices. Dual-root partitioning allows the SRX Series device to remain functional even if there is file system corruption and to facilitate easy recovery of the file system.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

SRX Series devices running Junos OS Release 9.6 or earlier support a single-root partitioning scheme where there is only one root partition. Because both the primary and backup Junos OS images are located on the same root partition, the system fails to boot if there is corruption in the root file system. The dual-root partitioning scheme guards against this scenario by keeping the primary and backup Junos OS images in two independently bootable root partitions. If the primary root partition becomes corrupted, the system can still boot from the backup Junos OS image located in the other root partition and remain fully functional.

SRX Series devices that ship with Junos OS Release 10.0 or later are formatted with dual-root partitions from the factory. SRX Series devices that are running Junos OS Release 9.6 or earlier can be formatted with dual-root partitions when they are upgraded to Junos OS Release 10.0 or later.



NOTE: Although you can install Junos OS Release 10.0 or later on SRX Series devices with the single-root partitioning scheme, we strongly recommend the use of the dual-root partitioning scheme.

This section contains the following topics:

- [Boot Media and Boot Partition on SRX Series Devices on page 106](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 106](#)
- [Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning on page 106](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices on page 108](#)
- [Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on page 109](#)

Boot Media and Boot Partition on SRX Series Devices

When the SRX Series device powers on, it tries to boot the Junos OS from the default storage media. If the device fails to boot from the default storage media, it tries to boot from the alternate storage media.

Table 19 provides information on the storage media available on SRX Series devices.

Table 19: Storage Media on SRX Series Devices

SRX Series Devices	Storage Media
SRX300, SRX320, and SRX340, and SRX345	<ul style="list-style-type: none"> eUSB disk (default; always present) USB storage device (alternate)
SRX550M	<ul style="list-style-type: none"> Internal CF (default; always present) USB storage device (alternate)

With the dual-root partitioning scheme, the SRX Series device first tries to boot Junos OS from the primary root partition and then from the backup root partition on the default storage media. If both primary and backup root partitions of a media fail to boot, then the SRX Series device tries to boot from the next available type of storage media. The SRX Series device remains fully functional even if it boots Junos OS from the backup root partition of the storage media.

Important Features of the Dual-Root Partitioning Scheme

The dual-root partitioning scheme has the following important features:

- The primary and backup copies of Junos OS images reside in separate partitions. The partition containing the backup copy is mounted only when required. With the single-root partitioning scheme, there is one root partition that contains both the primary and the backup Junos OS images.
- The **request system software add** command for a Junos OS package erases the contents of the other root partition. The contents of the other root partition will not be valid unless software installation is completed successfully.
- Add-on packages, such as **jais** or **jfirmware**, can be reinstalled as required after a new Junos OS image is installed.
- The **request system software rollback** command does not delete the current Junos OS image. It is possible to switch back to the image by issuing the **rollback** command again.
- The **request system software delete-backup** and **request system software validate** commands do not take any action.

Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning

The auto-snapshot feature repairs the corrupted primary root when the device reboots from the alternate root. This is accomplished by taking a snapshot of the alternate root onto the primary root automatically rather than manually from the CLI.

When this feature is enabled, and the device reboots from the alternate root (because of a corrupted primary root or power cycle during restart), the following actions take place:

1. A prominent message is displayed indicating a failure to boot from the primary root.

```
*****
**                                     **
**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE             **
**                                     **
**  It is possible that the primary copy of JUNOS failed to boot up          **
**  properly, and so this device has booted from the backup copy.            **
**                                     **
**  Please re-install JUNOS to recover the primary copy in case             **
**  it has been corrupted and if auto-snapshot feature is not               **
**  enabled.                                                                  **
**                                     **
*****
```

2. A system **boot from backup root** alarm is set. This is useful for devices that do not have console access.
3. A snapshot of the alternate root onto the primary root is made.
4. Once the snapshot is complete, the system **boot from backup root** alarm is cleared.

During the next reboot, the system determines the good image on the primary root and boots normally.



NOTE: We recommend performing the snapshot once all the processes start. This is done to avoid any increase in the reboot time.



NOTE:

- Auto-snapshot feature is supported on branch SRX Series devices.
- By default the auto-snapshot feature is disabled.
- If you do not maintain the same version of Junos OS in both partitions, ensure that the automatic snapshot feature remains disabled. Otherwise, if you have an earlier version of Junos OS in the alternate partition and the system reboots from the alternate root partition, the automatic snapshot feature causes the later Junos OS version to be replaced with the earlier version.
- When automatic snapshot is disabled and the system reboots from the alternate root partition, it triggers an alarm indicating that the system has rebooted from its alternate partition.

Enable this feature with the **set system auto-snapshot** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot.

Execute the **delete system auto-snapshot** command to delete all backed up data and disable auto-snapshot, if required.

Use the **show system auto-snapshot** command to check the auto-snapshot status.

When auto-snapshot is in progress, you cannot run a manual snapshot command concurrently and the following error message appears:

Snapshot already in progress. Please try after sometime.



NOTE: If you log into the device when the snapshot is in progress, the following banner appears: The device has booted from the alternate partition, auto-snapshot is in progress.

Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices

If the SRX Series Services Gateway is unable to boot from the primary Junos OS image, and boots up from the backup Junos OS image in the backup root partition, a message appears on the console at the time of login indicating that the device has booted from the backup Junos OS image.

```
login: user
```

```
Password:
```

```
*****
**
**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE  **
**
**  It is possible that the active copy of JUNOS failed to boot up **
**  properly, and so this device has booted from the backup copy.  **
**
**  Please re-install JUNOS to recover the active copy in case    **
**  it has been corrupted.                                         **
**
*****
```

Because the system is left with only one functional root partition, you should immediately restore the primary Junos OS image using one of the following methods:

- Install a new image using the CLI or J-Web user interface. The newly installed image will become the primary image, and the device will boot from it on the next reboot.

- Use a snapshot of the backup root partition by entering the **request system snapshot slice alternate** command. Once the primary root partition is recovered using this method, the device will successfully boot from the primary root partition on the next reboot. After the procedure, the primary root partition will contain the same version of Junos OS as the backup root partition.



NOTE: You can use the CLI command **request system snapshot slice alternate** to back up the currently running root file system (primary or secondary) to the other root partition on the system.

You can use this command to:

- Save an image of the primary root partition in the backup root partition when system boots from the primary root partition.
- Save an image of the backup root partition in the primary root partition when system boots from the backup root partition.



WARNING: The process of restoring the alternate root by using the CLI command **request system snapshot slice alternate** takes several minutes to complete. If you terminate the operation before completion, the alternate root might not have all required contents to function properly.

Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning



NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

To format the media with dual-root partitioning while upgrading to Junos OS Release 10.0 or later, use one of the following installation methods:

- Installation from the boot loader using a TFTP server. We recommend this if console access to the system is available and a TFTP server is available in the network. See [“Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server” on page 70](#)
- Installation from the boot loader using a USB storage device. We recommend this method if console access to the system is available and the system can be physically accessed to plug in a USB storage device. See [“Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device” on page 72](#)
- Installation from the CLI using the **partition** option. We recommend this method only if console access is not available. This installation can be performed remotely.



NOTE: After upgrading to Junos OS Release 10.0 or later, the U-boot and boot loader must be upgraded for the dual-root partitioning scheme to work properly.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110](#)

Example: Installing Junos OS on SRX Series Devices Using the Partition Option

This example shows how to install Junos OS Release 10.0 or later with the **partition** option.

- [Requirements on page 110](#)
- [Overview on page 110](#)
- [Configuration on page 111](#)
- [Verification on page 113](#)

Requirements

Before you begin, back up any important data.

Overview

This example formats the internal media and installs the new Junos OS image on the media with dual-root partitioning. Reinstall the Release 10.0 or later image from the CLI using the **request system software add** command with the **partition** option. This copies the image to the device, and then reboots the device for installation. The device boots up with the Release 10.0 or later image installed with the dual-root partitioning scheme. When the **partition** option is used, the format and install process is scheduled to run on the next reboot. Therefore, we recommend that this option be used together with the **reboot** option.



NOTE: The process might take 15 to 20 minutes. The system is not accessible over the network during this time.



WARNING: Using the partition option with the **request system software add** command erases the existing contents of the media. Only the current configuration is preserved. You should back up any important data before starting the process.



NOTE: Partition install is supported on the default media on SRX300, SRX320, 340, and SRX345 devices (internal NAND flash) and *not* supported on the alternate media (USB storage key).

In this example, add the software package `junos-srxsme-10.0R2-domestic.tgz` with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **partition** option to format and re-partition the media before installation.
- **reboot** option to reboots the device after installation is completed.

Configuration

CLI Quick Configuration

To quickly install Junos OS Release 10.0 or later with the **partition** option, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy
no-validate partition reboot
```

GUI Step-by-Step Procedure

To install Junos OS Release 10.0 or later with the **partition** option:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Package page, specify the FTP or HTTP server, file path, and software package name. Type the full address of the software package location on the FTP (<ftp://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz>) or HTTP server (<http://hostname/pathname/junos-srxsme-10.0R2-domestic.tgz>).



NOTE: Specify the username and password, if the server requires one.

3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package.
5. Select the **Format and re-partition the media before installation** check box to format the internal media with dual-root partitioning.
6. Click **Fetch and Install Package**. The software is activated after the device reboots.

This formats the internal media and installs the new Junos OS image on the media with dual-root partitioning.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To install Junos OS Release 10.0 or later with the **partition** option:

1. Upgrade the device to Junos OS Release 10.0 or later using the CLI.
2. After the device reboots, upgrade the boot loader to the latest version. See [“Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices” on page 66](#).
3. Reinstall the Release 10.0 or later image.

```
user@host>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy
no-validate partition reboot
Copying package junos-srxsme-10.0R2-domestic.tgz to var/tmp/install
Rebooting ...
```

Results From configuration mode, confirm your configuration by entering the **show system storage partitions** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Sample output on a system with single root partitioning:

```
user@host> show system storage partitions

Boot Media: internal (da0)

Partitions Information:
  Partition  Size  Mountpoint
    s1a      898M  /
    s1e       24M  /config
    s1f        61M  /var
```

Sample output on a system with dual-root partitioning:

```
user@host> show system storage partitions

Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size  Mountpoint
    s1a      293M  altroot
    s2a      293M  /
    s3e       24M  /config
    s3f      342M  /var
    s4a       30M  recovery
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Partitioning Scheme Details on page 113](#)

Verifying the Partitioning Scheme Details

Purpose Verify that the partitioning scheme details on the SRX Series device were configured.

Action From operational mode, enter the **show system storage partitions** command.

Related Documentation • [Dual-Root Partitioning Scheme on SRX Series Devices on page 105](#)

CHAPTER 8

Upgrading Software

- [Upgrading Software Packages on page 116](#)
- [Upgrading to 64-bit Junos OS on page 119](#)
- [Upgrading Routers Using Unified ISSU on page 122](#)
- [Understanding Nonstop Software Upgrade on EX Series Switches on page 123](#)
- [Upgrading Software by Using Automatic Software Download on page 129](#)
- [Verifying That Automatic Software Download Is Working Correctly on page 131](#)
- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)
- [Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis on page 136](#)
- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 154](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 155](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 156](#)

Upgrading Software Packages



NOTE: When you install individual software packages, the following notes apply:

- When upgrading from Junos OS Release 8.2 or earlier to Junos OS Release 8.5, use the `system software add <image> no-validate` command option.
- Only use the `jinstall` Junos OS image when upgrading or downgrading to or from Junos OS Release 8.5. Do not use the `jbundle` image.
- Before upgrading to Junos OS Release 8.5, ensure that the routing platform's CompactFlash card is 256 MB or larger to avoid disk size restrictions. (M7i routers without a CompactFlash card are excluded.)



NOTE: If you are upgrading a Routing Engine on a PTX Series router to run Junos OS Release 13.2R2 and later, and then make that Routing Engine the master Routing Engine, then the master Routing Engine reports a major alarm `CB 0/1 ESW PFE Port Fail` even though the Control Board's Ethernet switch links are up and running on both the master and the backup Routing Engines. This is because the backup Routing Engine is still on Junos OS Release 13.2R1 or earlier. The alarm is cleared after you have completed the upgrade of Junos OS on the backup Routing Engine.

```
User@router# show chassis alarms
2 alarms currently active
Alarm time Class Description
2014-10-15 00:44:31 BST Major CB 0 ESW PFE Port Fail
2014-10-15 00:42:42 BST Minor Backup RE Active
```

To upgrade an individual Junos OS package, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site at <http://www.juniper.net/support/>. For information about downloading software packages, see ["Downloading Software" on page 48](#).



NOTE: We recommend that you upgrade all individual software packages using an out-of-band connection from the console or management Ethernet interface, because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's CompactFlash card, and the `/altroot` and `/altconfig` file systems are on the router's hard disk or solid-state drive (SSD).



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.



NOTE: High-end SRX Series devices, the root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's CompactFlash card, and the `/altroot` and `/altconfig` file systems are on the router's hard disk or solid-state drive (SSD).



NOTE: This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.

3. If you are copying multiple software packages to the router, copy them to the `/var/tmp` directory on the hard disk or solid-state drive (SSD):

```
user@host> file copy ftp://username :prompt@ftp.hostname
.net/filename/var/tmp/filename
```

4. Add the new software package:

- To add an individual software package:

```
user@host> request system software add /var/tmp/ installation-package validate
```

installation-package is the full URL to the file.



NOTE: Warning: For high-end SRX Series devices, do not include the `re0 | re1` option when you install a package using the `request system software add` command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package is the same. In such cases, the package gets deleted after a successful upgrade.

If you are upgrading more than one package at the same time, add `jbase` first. If you are using this procedure to upgrade all packages at once, add them in the following order:

```
user@host> request system software add /var/tmp/jbase-release-signed.tgz
```

```
user@host> request system software add /var/tmp/jkernel-release-signed.tgz
```

```

user@host> request system software add /var/tmp/jpfe-release-signed.tgz
user@host> request system software add /var/tmp/jdocs-release-signed.tgz
user@host> request system software add /var/tmp/jweb-release-signed.tgz
user@host> request system software add /var/tmp/jroute-release-signed.tgz
user@host> request system software add /var/tmp/jcrypto-release-signed.tgz

```

- For M Series, MX Series, and T Series routers and Branch SRX Series firewall filters running Junos OS Release 12.2 and above, you can add more than one software package at the same time. To add multiple software packages:

```

user@host> request system software add set /var/tmp/
installation-package/var/tmp/ installation-package validate

```

installation-package can be any of the following:

- A list of installation packages, each separated by a blank space. For example,

```

user@host> request system software add set /var/tmp/
jinstall-10.2R1.8-domestic-signed.tgz /var/tmp/jtools*.tgz validate

```

- The full URL to the directory or tar file containing the list of installation packages.

Use the **request system software add set** command to retain any SDK configuration by installing the SDK add-on packages along with the core Junos OS installation package.



WARNING: Do not include the *re0* | *re1* option when you install a package using the **request system software add** command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package are the same. In such cases, the package gets deleted after a successful upgrade.

The system might display the following message:

```
pkg_delete: couldn't entirely delete package
```

This message indicates that someone manually deleted or changed an item that was in a package. You do not need to take any action; the package is still properly deleted.

For more information about the **request system software add** command, see the [CLI Explorer](#).

5. Reboot the router to start the new software:

```
user@host> request system reboot
```

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the **request system snapshot** command to back up the new software:

```
user@host> request system snapshot
```



NOTE: On an ACX router, you must issue the `request system snapshot slice alternate` command.

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's CompactFlash card, and the `/altroot` and `/altconfig` file systems are on the router's hard disk or solid-state drive (SSD).



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.

Upgrading to 64-bit Junos OS

Just like any other operating system, the 64-bit version of Junos OS can address more memory than the 32-bit version of the operating system. In order to support larger Routing Engine memory sizes, an upgrade from the 32-bit to the 64-bit Junos OS running on the Routing Engine hardware is necessary. The upgrade path is relatively straightforward and another form of Routing Engine hardware and software upgrade. However, there are three different and distinct Routing Engine configurations that must be taken into account when upgrading to the 64-bit Junos OS. This topic covers all three.

The In Service Software Upgrade (ISSU) procedure is not supported while upgrading from the 32-bit version of Junos OS to the 64-bit version of Junos OS. The upgrade process involves some downtime, so traffic will be affected.



NOTE: The 64-bit version of Junos OS is not supported on every Routing Engine. To determine whether your router and Routing Engine support a 64-bit version of Junos OS, see *Supported Routing Engines by Router*.

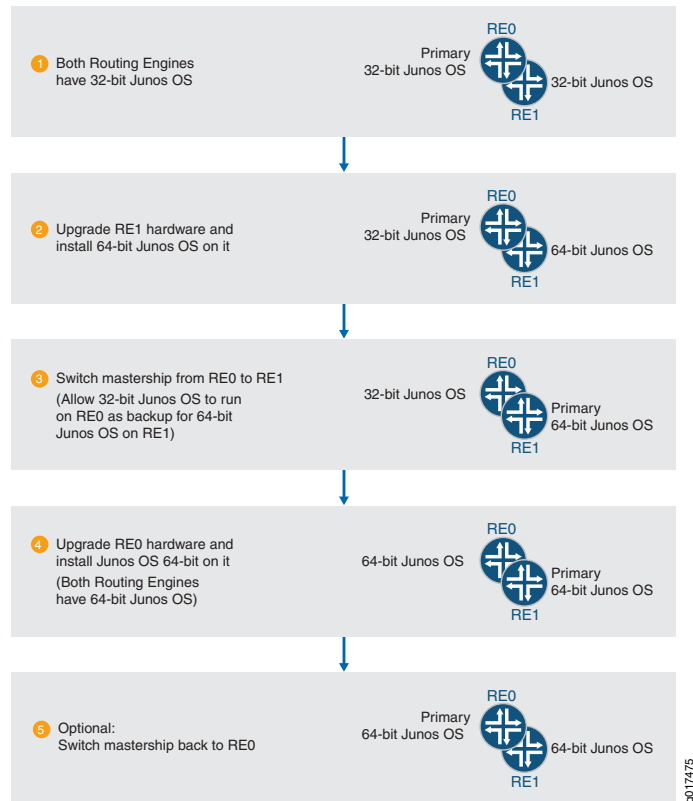
Before you begin, you must have:

- A properly configured and functional router
- One or two Routing Engines installed that support the 64-bit Junos OS
- Decided to allow single Routing Engines systems to use either slot 0 or slot 1 as master or not (this decision will determine which upgrade path to follow for single Routing Engine systems)

When you upgrade a Routing Engine to the 64-bit Junos OS, you can support larger Routing Engine memory sizes. However, the exact procedure depends on whether there are one or two Routing Engines installed. For systems with a single Routing Engine, the procedure varies based on whether the master Routing Engine must always be in slot 0 or not.

To upgrade a system with two Routing Engines, refer to [Figure 7](#) and perform the following steps:

Figure 7: Upgrading to the 64-bit Junos OS with Dual Routing Engines

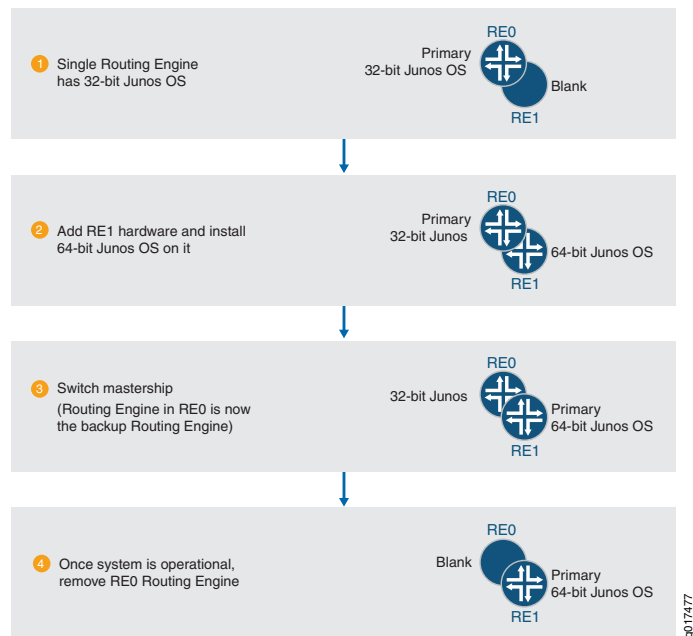


1. In the initial state, both Routing Engines are running the 32-bit Junos OS, and slot 0 has the master Routing Engine.
2. Upgrade the slot 1 Routing Engine hardware and install the 64-bit Junos OS.
For instructions on replacing a Routing Engine, see the hardware guide for your router.
3. Switch the master Routing Engine from slot 0 to slot 1 (allow the 32-bit Junos OS to co-exist with the 64-bit Junos OS).
4. Upgrade the slot 0 routing engine hardware and install the 64-bit Junos OS.
5. Both Routing Engines now run the 64-bit Junos OS. Optionally, you can switch the master Routing Engine back to slot 0.



NOTE: Mixing the 32-bit Junos OS with the 64-bit Junos OS is only supported temporarily during the upgrade process. Mixing the two operating systems is not supported for normal operations.

Figure 8: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master in Either Slot)

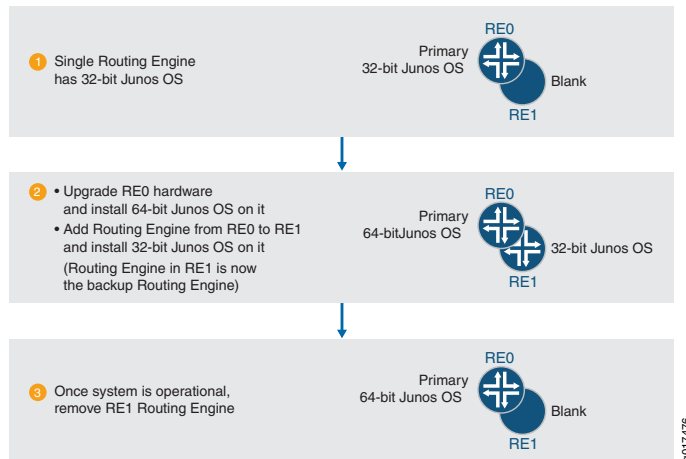


To upgrade a system with a single Routing Engine, where the master Routing Engine can be in either slot 0 or slot 1, refer to [Figure 7](#) and perform the following steps:

1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the upgraded Routing Engine hardware in slot 1 and install the 64-bit Junos OS.
For instructions on installing a Routing Engine, see the hardware guide for your router.
3. When the 64-bit Junos OS is configured properly, remove the slot 0 Routing Engine running the 32-bit Junos OS.

To upgrade a system with a single Routing Engine, where the master Routing Engine must be in slot 0, refer to [Figure 9](#) and perform the following steps:

Figure 9: Upgrading to the 64-bit Junos OS with a Single Routing Engine (Master Must Be in Slot 0)



1. In the initial state, the slot 0 Routing Engine is running the 32-bit Junos OS and slot 1 is blank.
2. Install the slot 0 Routing Engine hardware in slot 1. Install the upgraded Routing Engine hardware in slot 0 and install the 64-bit Junos OS.
For instructions on installing a Routing Engine, see the hardware guide for your router.
3. When the 64-bit Junos OS is configured properly, remove the slot 1 routing engine running the 32-bit Junos OS.

Related Documentation

- [Checklist for Reinstalling Junos OS on page 187](#)

Upgrading Routers Using Unified ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified ISSU is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled.

For additional information about using unified ISSU, see the *Junos OS High Availability Library for Routing Devices*.

For additional information about using unified ISSU on SRX Series devices, see the [Junos OS Chassis Cluster Library for Security Devices](#).

Related Documentation

- [Upgrading Individual Software Packages on page 116](#)

Understanding Nonstop Software Upgrade on EX Series Switches

Nonstop software upgrade (NSSU) enables you to upgrade the software running on Juniper Networks EX Series Ethernet Switches with redundant Routing Engines and all member switches in EX Series Virtual Chassis by using a single command and with minimal network traffic disruption during the upgrade.

NSSU is supported on the following platforms:

- EX3300 Virtual Chassis
- EX4200 Virtual Chassis
- EX4300 Virtual Chassis
- EX4500 Virtual Chassis
- EX4550 Virtual Chassis
- All mixed Virtual Chassis composed of EX4200, EX4500, and EX4550 switches
- EX6200 switches
- EX8200 switches
- EX8200 Virtual Chassis

Performing an NSSU provides these benefits:

- No disruption to the control plane—An NSSU takes advantage of graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) to ensure no disruption to the control plane. During the upgrade process, interface, kernel, and routing protocol information is preserved.
- Minimal disruption to network traffic—An NSSU minimizes network traffic disruption by:
 - Upgrading line cards one at a time in an EX6200 switch, EX8200 switch, or EX8200 Virtual Chassis, permitting traffic to continue to flow through the line cards that are not being upgraded.
 - Upgrading member switches one at a time in an EX3300, EX4200, EX4300, EX4500, or mixed Virtual Chassis, permitting traffic to continue to flow through the members that are not being upgraded.

To achieve minimal disruption to traffic, you must configure link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards or Virtual Chassis members. When one member link of a LAG is down, the remaining links are up, and traffic continues to flow through the LAG.



NOTE: Because NSSU upgrades the software on each line card or on each Virtual Chassis member one at a time, an upgrade using NSSU can take longer than an upgrade using the `request system software add` command.

For EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can reduce the amount of time an upgrade takes by configuring line-card upgrade groups. The line cards in an upgrade group are upgraded simultaneously, reducing the amount of time it takes to complete an upgrade. See *Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)*.

This topic covers:

- [Requirements for Performing an NSSU on page 124](#)
- [How an NSSU Works on page 125](#)
- [NSSU Limitations on page 128](#)
- [NSSU and Junos OS Release Support on page 128](#)
- [Overview of NSSU Configuration and Operation on page 129](#)

Requirements for Performing an NSSU

The following requirements apply to all switches and Virtual Chassis:

- All Virtual Chassis members and all Routing Engines must be running the same Junos OS release.
- Graceful Routing Engine switchover (GRES) must be enabled.
- Nonstop active routing (NSR) must be enabled.



NOTE: Although nonstop bridging (NSB) does not have to be enabled to perform an NSSU, we recommend enabling NSB before performing an NSSU. Enabling NSB ensures that all NSB-supported Layer 2 protocols operate seamlessly during the Routing Engine switchover that is part of the NSSU. See *Configuring Nonstop Bridging on EX Series Switches (CLI Procedure)*.

- For minimal traffic disruption, you must define link aggregation groups (LAGs) such that the member links reside on different Virtual Chassis members or on different line cards.

The following are requirements for EX3300, EX4200, EX4300, EX4500, and mixed Virtual Chassis:

- The Virtual Chassis members must be connected in a ring topology so that no member is isolated as a result of another member being rebooted. This topology prevents the Virtual Chassis from splitting during an NSSU.
- The Virtual Chassis master and backup must be adjacent to each other in the ring topology. Adjacency permits the master and backup to always be in sync, even when the switches in linecard roles are rebooting.
- The Virtual Chassis must be preprovisioned so that the linecard role has been explicitly assigned to member switches acting in a linecard role. During an NSSU, the Virtual Chassis members must maintain their roles—the master and backup must maintain their master and backup roles (although mastership will change), and the remaining switches must maintain their linecard roles.
- A two-member Virtual Chassis must have **no-split-detection** configured so that the Virtual Chassis does not split when an NSSU upgrades a member.



NOTE: For the EX4300 Virtual Chassis, you should enable the `vcp-no-hold-time` statement at the `[edit virtual-chassis]` hierarchy level before performing a software upgrade using NSSU. If you do not enable the `vcp-no-hold-time` statement, the Virtual Chassis may split during the upgrade. A split Virtual Chassis can cause disruptions to your network, and you may have to manually reconfigure your Virtual Chassis after the NSSU if the split and merge feature was disabled. For more information about a split Virtual Chassis, see *Understanding Split and Merge in a Virtual Chassis*

How an NSSU Works

This section describes what happens when you request an NSSU on these switches and Virtual Chassis:

- [EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis on page 125](#)
- [EX6200 and EX8200 Switches on page 126](#)
- [EX8200 Virtual Chassis on page 127](#)

EX3300, EX4200, EX4300, EX4500, and Mixed Virtual Chassis

When you request an NSSU on an EX3300, EX4200, EX4300, EX4500, or mixed Virtual Chassis:

1. The Virtual Chassis master verifies that:
 - The backup is online and running the same software version.
 - Graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) are enabled.
 - The Virtual Chassis has a preprovisioned configuration.
2. The master installs the new software image on the backup and reboots it.
3. The master resynchronizes the backup.

4. The master installs the new software image on member switches that are in the linecard role and reboots them, one at a time. The master waits for each member to become online and active before starting the software upgrade on the next member.
5. When all members that are in the linecard role have been upgraded, the master performs a graceful Routing Engine switchover, and the upgraded backup becomes the master.
6. The software on the original master is upgraded and the original master is automatically rebooted. After the original master has rejoined the Virtual Chassis, you can optionally return control to it by requesting a graceful Routing Engine switchover.

EX6200 and EX8200 Switches

When you request an NSSU on a standalone switch with redundant Routing Engines:

1. The switch verifies that:
 - Both Routing Engines are online and running the same software version.
 - Both Routing Engines have sufficient storage space for the new software image.
 - Graceful Routing Engine switchover and nonstop active routing are enabled.
2. The switch installs the new software image on the backup Routing Engine and reboots it.
3. The switch resynchronizes the backup Routing Engine to the master Routing Engine.
4. The line cards in the first upgrade group (or the line card in slot 0, if no upgrade groups are defined) download the new image and then restart. Traffic continues to flow through the line cards in the other upgrade groups during this process.
5. When line cards restarted in Step 4 are online again, the line cards in the next upgrade group download the new image and restart. This process continues until all online line cards have restarted with the new software.



NOTE: If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.

6. The switch performs a graceful Routing Engine switchover, so that the upgraded backup Routing Engine becomes the master.
7. The switch installs the new software on the original master Routing Engine.

To complete the upgrade process, the original master Routing Engine must be rebooted. You can do so manually or have the switch perform an automatic reboot by including the **reboot** option when you request the NSSU. After the original master has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.
8. (EX6200 switch only) The original master Routing Engine reboots to complete the software upgrade.



NOTE: To complete the upgrade process on an EX8200 switch, you must intervene to reboot the original master Routing Engine. You can reboot the original master Routing Engine manually or have the switch perform an automatic reboot by including the `reboot` option when you request the NSSU.

9. (Optional) After the original master has been rebooted, you can return control to it by requesting a graceful Routing Engine switchover.

The switch can maintain normal operations with either Routing Engine acting as the master Routing Engine after the software upgrade, so you only have to perform this switchover if you want to return Routing Engine control to the original master Routing Engine.

EX8200 Virtual Chassis

When you request an NSSU on an EX8200 Virtual Chassis:

1. The master external Routing Engine verifies that:
 - It has a backup external Routing Engine that is online.
 - All Virtual Chassis members have redundant Routing Engines and the Routing Engines are online.
 - All Routing Engines are running the same software version.
 - All Routing Engines have sufficient storage space for the new software image.
 - Graceful Routing Engine switchover and nonstop active routing (NSR) are enabled.
2. The master external Routing Engine installs the new software image on the backup external Routing Engine and reboots it.
3. The backup external Routing Engine resynchronizes with the master external Routing Engine.
4. The master external Routing Engine installs the new software on the backup Routing Engines in the member switches and reboots the backup Routing Engines.
5. When the reboot of the backup Routing Engines complete, the line cards in the first upgrade group download the new image and then restart. (If no upgrade groups are defined, the line card in slot 0 of member 0 downloads the new image and restarts.) Traffic continues to flow through the line cards in the other upgrade groups during this process.
6. When line cards restarted in Step 5 are online again, the line cards in the next upgrade group (or the next sequential line card) download the new image and restart. This process continues until all online line cards have restarted with the new software.



NOTE: If you have taken a line card offline with the CLI before you start the NSSU, the line card is not restarted and remains offline.

7. The new software image is installed on the master Routing Engines, both external and internal.
8. The member switches perform a graceful Routing Engine switchover, so that the upgraded backup Routing Engines become masters.
9. The master external Routing Engine performs a graceful Routing Engine switchover so that the backup external Routing Engine is now the master.

To complete the upgrade process, the original master Routing Engines, both external and internal, must be rebooted. You can do so manually by establishing a console connection to each Routing Engine or have the reboot performed automatically by including the **reboot** option when you request the NSSU. After the original master external Routing Engine has been rebooted, you can optionally return control to it by requesting a graceful Routing Engine switchover.

NSSU Limitations

You cannot use an NSSU to downgrade the software—that is, to install an earlier version of the software than is currently running on the switch. To install an earlier software version, use the **request system software add** command.

You cannot roll back to the previous software version after you perform an upgrade using NSSU. If you need to rollback to the previous software version, you can do so by rebooting from the alternate root partition if you have not already copied the new software version into the alternate root partition.

NSSU and Junos OS Release Support

A Virtual Chassis must be running a Junos OS release that supports NSSU before you can perform an NSSU. If a Virtual Chassis is running a software version that does not support NSSU, use the **request system software add** command.

Table 20 lists the EX Series switches and Virtual Chassis that support NSSU and the Junos OS release at which they began supporting it.

Table 20: Platform and Release Support for NSSU

Platform	Junos OS Release
EX3300 Virtual Chassis	12.2 or later
EX4200 Virtual Chassis	12.1 or later
EX4300 Virtual Chassis	13.2X51-D20 or later
EX4500 Virtual Chassis	12.1 or later
EX4550 Virtual Chassis	12.2 or later
Mixed EX4200 and EX4500 Virtual Chassis	12.1 or later
Mixed EX4200 and EX4550 Virtual Chassis	12.2 or later

Table 20: Platform and Release Support for NSSU (*continued*)

Platform	Junos OS Release
Mixed EX4200, EX4500, and EX4550 Virtual Chassis	12.2 or later
Mixed EX4500 and EX4550 Virtual Chassis	12.2 or later
EX6200 switch	12.2 or later
EX8200 switch	10.4 or later
EX8200 Virtual Chassis	11.1 or later

Overview of NSSU Configuration and Operation

You must ensure that the configuration of the switch or Virtual Chassis meets the requirements described in [“Requirements for Performing an NSSU” on page 124](#). NSSU requires no additional configuration.

For EX6200 switches, EX8200 switches, and EX8200 Virtual Chassis, you can optionally configure line-card upgrade groups using the CLI. See *Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches*.

You perform an NSSU by executing the **request system software nonstop-upgrade** command. For detailed instructions on how to perform an NSSU, see the topics in Related Documentation.

Related Documentation

- *Upgrading Software on an EX3300, EX4200, EX4300, EX4500 and EX4550 Virtual Chassis, and Mixed Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)*
- *Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)*
- *Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)*
- *Configuring Nonstop Active Routing on Switches*
- *Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure)*
- *Example: Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade on EX Series Switches*

Upgrading Software by Using Automatic Software Download

The automatic software download feature uses the Dynamic Host Configuration Protocol (DHCP) message exchange process to download and install software packages. You configure the automatic software download feature on switches that act as DHCP clients. You must enable automatic software download on a switch before the software upgrade can occur.

You configure a path to a software package file on the DHCP server. The server communicates the path to the software package file through DHCP server messages.

If you enable automatic software download, the DHCP client switch compares the software package name in the DHCP server message with the name of the software package that booted the switch. If the software packages are different, the DHCP client switch downloads and installs the software package specified in the DHCP server message.

Before you upgrade software by using automatic software download, ensure that you have configured DHCP services for the switch, including configuring a path to a boot server and a boot file.

To configure a path to a boot server and a boot file:

1. Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This configuration is equivalent to DHCP Option 66:

```
[edit system services dhcp]
user@switch# set boot-server (address | hostname)
```

2. Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete the DHCP setup. This configuration is equivalent to DHCP Option 67:

```
[edit system services dhcp]
user@switch# set boot-file filename
```

To enable automatic software download on a switch that acts as a DHCP client:

```
[edit chassis]
user@switch# set auto-image-upgrade
```

After automatic software download is enabled on your DHCP client switch and after DHCP services are enabled on your network, an automatic software download can occur at any time as part of the DHCP message exchange process.

If an automatic software download occurs, you see the following message on the switch:

```
Auto-image upgrade started
On successful installation system will reboot automatically
```

The switch reboots automatically to complete the upgrade.

Related Documentation

- [Verifying That Automatic Software Download Is Working Correctly on page 131](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)
- [Configuring DHCP Services \(J-Web Procedure\)](#)

Verifying That Automatic Software Download Is Working Correctly

Purpose Verify that the automatic software download feature is working correctly.

Action Use the `show system services dhcp client interface-name` command to verify that the automatic software download feature has been used to install a software package.

```
user@switch> show system services dhcp client ge-0/0/1.0
Logical Interface Name      ge-0/0/1.0
Hardware address           00:0a:12:00:12:12
Client Status               bound
Vendor Identifier           ether
Server Address              10.1.1.1
Address obtained            10.1.1.89
Lease Obtained at           2009-08-20 18:13:04 PST
Lease Expires at            2009-08-22 18:13:04 PST

DHCP Options :
Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
Name: server-identifier, Value: 10.1.1.1
Name: router, Value: [ 10.1.1.80 ]
Name: boot-image,
Value: jinstall-ex-4200-9.6R1.5-domestic-signed.tgz
Name: boot-image-location,
Value: 10.1.1.25:/bootfiles/
```

Meaning The output from this command shows the name and location of the software package under DHCP options when automatic software download was last used to install a software package. The sample output in DHCP options shows that the last DHCP server message to arrive on the DHCP client had a boot server address of 192.168.1.165 and a boot file named jinstall-ex-4200-9.6R1.5-domestic-signed.tgz. If automatic software download was enabled on this client switch during the last DHCP message exchange, these values were used by the switch to upgrade the software.

Related Documentation

- [Upgrading Software by Using Automatic Software Download on page 129](#)

Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch

Before or after upgrading or downgrading Junos OS, you might need to verify the Junos OS version. You might also need to verify the boot loader software version if you are upgrading to or downgrading from a release that supports resilient dual-root partitions (Junos OS Release 10.4R3 and later).

This topic includes:

- [Verifying the Number of Partitions and File System Mountings on page 132](#)
- [Verifying the Loader Software Version on page 132](#)
- [Verifying Which Root Partition Is Active on page 133](#)
- [Verifying the Junos OS Version in Each Root Partition on page 134](#)

Verifying the Number of Partitions and File System Mountings

Purpose Between Junos OS Release 10.4R2 and Release 10.4R3, upgrades were made to further increase resiliency of root partitions, which required reformatting the disk from three partitions to four partitions. If your switch is running Release 10.4R2 or earlier, it has three partitions, and if it is running Release 10.4R3 or later, it has four partitions.

Action Verify how many partitions the disk has, as well as where each file system is mounted, by using the following command:

```
user@switch> show system storage
fpc0:
```

```
-----
Filesystem Size Used Avail Capacity Mounted on
/dev/da0s1a 184M 124M 45M 73% /
devfs 1.0K 1.0K 0B 100% /dev
/dev/md0 37M 37M 0B 100% /packages/mnt/jbase
/dev/md1 18M 18M 0B 100%
/packages/mnt/jcrypto-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md2 6.1M 6.1M 0B 100%
/packages/mnt/jdocs-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md3 154M 154M 0B 100%
/packages/mnt/jkernel-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md4 23M 23M 0B 100%
/packages/mnt/jpfe-ex42x-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md5 46M 46M 0B 100%
/packages/mnt/jroute-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md6 28M 28M 0B 100%
/packages/mnt/jswitch-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md7 22M 22M 0B 100%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md8 126M 10.0K 116M 0% /tmp
/dev/da0s3e 123M 632K 112M 1% /var
/dev/da0s3d 369M 20K 339M 0% /var/tmp
/dev/da0s4d 62M 62K 57M 0% /config
/dev/md9 118M 12M 96M 11% /var/rundb
procfs 4.0K 4.0K 0B 100% /proc
/var/jail/etc 123M 632K 112M 1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/etc
/var/jail/run 123M 632K 112M 1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/run
/var/jail/tmp 123M 632K 112M 1%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/tmp
/var/tmp 369M 20K 339M 0%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/var/tmp/uploads
devfs 1.0K 1.0K 0B 100%
/packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081/jail/dev
```

Meaning The presence of the partition name containing **s4d** indicates that there is a fourth slice. If this were a three-slice partition scheme, in place of **s1a**, **s3e**, **s3d**, and **s4d**, you would see **s1a**, **s1f**, **s2a**, **s2f**, **s3d**, and **s3e** and you would not see **s4d**.

Verifying the Loader Software Version

Purpose For the special case of upgrading from Junos OS Release 10.4R2 or earlier to Release 10.4R3 or later, you must upgrade the loader software.

Action For EX Series switches except EX8200 switches:

```
user@switch> show chassis firmware
Part          Type      Version
FPC 0         uboot     U-Boot 1.1.6 (Jan  3 2011 - 16:14:58) 1.0.0

              loader   FreeBSD/PowerPC U-Boot bootstrap loader 2.4
```

For EX8200 switches:

```
user@switch> show chassis firmware
Part          Type      Version
FPC 0         uboot     U-Boot 1.1.6 (Jan  3 2011 - 16:14:58) 3.5.0

              loader   FreeBSD/PowerPC U-Boot bootstrap loader 2.4
```

Meaning For EX Series switches other than EX8200 switches, with Junos OS Release 10.4R3 or later installed:

- If there is version information following the timestamp for **U-Boot** (1.0.0 in the preceding example), then the loader software does not require upgrading.
- If there is no version number following the timestamp for **U-boot**, then the loader software requires upgrading.



NOTE: If the software version is Release 10.4R2 or earlier, no version number is displayed following the timestamp for **U-boot**, regardless of the loader software version installed. If you do not know whether you have installed the new loader software, we recommend that you upgrade the loader software when you upgrade the software version.

For EX8200 switches, if the version number following the timestamp for **U-Boot** is earlier than **3.5.0**, you must upgrade the loader software when you upgrade the software version.

Verifying Which Root Partition Is Active

Purpose Switches running Release 10.4R3 or later have resilient dual-root partition functionality, which includes the ability to boot transparently from the inactive partition if the system fails to boot from the primary root partition.

You can verify which root partition is active using the following command:

Action user@switch> `show system storage partitions`
fpc0:

```
-----
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:
  Partition  Size  Mountpoint
  s1a        184M  /
  s2a        184M  altroot
  s3d        369M  /var/tmp
  s3e        123M  /var
  s4d         62M  /config
  s4e                unused (backup config)
```

Meaning The **Currently booted from:** field shows which root partition is active.

Verifying the Junos OS Version in Each Root Partition

Purpose Each switch contains two root partitions. We recommend that you copy the same Junos OS version in each partition when you upgrade. In Junos OS Release 10.4R2 and earlier, you might choose to have different Junos OS release versions in each partition. You might have different versions during a software upgrade and before you have finished verifying the new software installation. To enable a smooth reboot if corruption is found in the primary root file system, ensure that the identical Junos OS images are in each root partition. For Release 10.4R2 and earlier, you must manually reboot the switch from the backup root partition. However, for Release 10.4R3 and later, the switch reboots automatically from the backup root partition if it fails to reboot from the active root partition.

Action Verify whether both root partitions contain the same image by using the following command:

```
user@switch> show system snapshot media internal
Information for snapshot on      internal (/dev/da0s1a) (backup)
Creation date: Jan 11 03:02:59 2012
JUNOS version on snapshot:
  jbase   : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
Information for snapshot on      internal (/dev/da0s2a) (primary)
Creation date: Mar 6 02:24:08 2012
JUNOS version on snapshot:
  jbase   : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

Meaning The command shows which Junos OS version is installed on each media partition. Verify that the same version is installed on both partitions.

- Related Documentation**
- [Troubleshooting Software Installation on page 265](#)
 - [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 268](#)
 - [Understanding Resilient Dual-Root Partitions on Switches on page 95](#)
 - [Resilient Dual-Root Partitions Frequently Asked Questions on page 99](#)

Upgrading the Loader Software on the Line Cards in a Standalone EX8200 Switch or an EX8200 Virtual Chassis

You are almost never required to upgrade the loader software on the line cards in an EX8200 switch.

Upgrading the loader software version for a line card is not a requirement to complete any software upgrade. In rare cases, a line card might go offline immediately after a software upgrade because the loader software version on the line card requires an upgrade to become compatible with the upgraded Junos OS. You can upgrade the loader software on the line cards as a best practice to avoid this problem and other less severe issues.

The loader software on any line card in an EX8200 switch is updated using the same loader software package that upgrades the EX8200 Routing Engine loader software. The line card software loader contains two banks, each with a single loader software version. This procedure is used to upgrade the loader software for both banks of a line card in a standalone EX8200 switch or an EX8200 Virtual Chassis.



NOTE: If you are upgrading Junos OS, the Routing Engine loader software, and the line card loader software, we recommend that you upgrade in this order: Junos OS, line card loader software, Routing Engine loader software.

1. Determine the version of the loader software for the line cards:

```

user@switch> show chassis firmware
Part      Type      Version
FPC 6     U-Boot    U-Boot 1.1.6 (Jan 13 2009 - 06:55:22) 2.3.0
          loader  FreeBSD/PowerPC U-Boot bootstrap loader 2.2
FPC 7     U-Boot    U-Boot 1.1.6 (Jan 13 2009 - 06:55:22) 2.3.0
          loader  FreeBSD/PowerPC U-Boot bootstrap loader 2.2
Routing Engine 0 U-Boot    U-Boot 1.1.6 (Mar 11 2011 - 04:29:01) 3.5.0
          loader  FreeBSD/PowerPC U-Boot bootstrap loader 2.4
Routing Engine 1 U-Boot    U-Boot 1.1.6 (Mar 11 2011 - 04:29:01) 2.3.0
          loader  FreeBSD/PowerPC U-Boot bootstrap loader 2.4

```



NOTE: On an EX8200 Virtual Chassis, you cannot execute the `show chassis firmware` command on the master external Routing Engine. You must execute this command on each member switch:

1. From the master external Routing Engine, start a shell session on the member switch. For example:

```
user@external-routing-engine> request session member 0
```

2. Enter the CLI and execute the `show chassis firmware` command.
3. Repeat these steps for the other member switch.

The loader software version appears after the timestamp for **U-Boot 1.1.6**. In the preceding example, the version is **2.3.0**. Ignore the U-Boot version number (1.1.6); it has nothing to do with the loader software version that you need to determine.

If the loader software version is earlier than **3.5.0** for any **FPC**, you should consider upgrading the loader software for that line card.

2. Download the loader software package from the Juniper Networks website and place the software package on an internal software distribution site or in a local directory on the switch. We recommend using `/var/tmp` as the local directory on the switch.



NOTE: To obtain the loader software package, see the Download Software page at <http://www.juniper.net/support/downloads/junos.html>. Click on the version, then the Software tab, and then the name of the software install package. In the pop-up Alert box, click the link to the PSN document.

3. Disable graceful Routing Engine switchover (GRES) and nonstop active routing (NSR), if enabled. Commit the configuration:

```

user@switch# deactivate chassis redundancy graceful-switchover
user@switch# deactivate routing-options nonstop-routing
user@switch# commit synchronize

```

4. Install the loader package:

```
user@switch> request system software add package
```

Replace **package** with one of the following paths:

- For a software package in the `/var/tmp` directory on the switch or external Routing Engine—`/var/tmp/package.tgz`
- For a software package on a remote server:
 - `ftp://hostname/pathname/package.tgz`
 - `http://hostname/pathname/package.tgz`

where *package.tgz* is, for example, `jloader-ex-8200-11.3build-signed.tgz`.

5. Upgrade the loader software.

- To upgrade the loader software for a line card on a standalone EX8200 switch:

```
user@switch> request system firmware upgrade fpc slot slot-number
Firmware upgrade initiated....
Please wait for ~2mins for upgrade to complete....
```

- To upgrade the loader software for a line card on an EX8200 member switch in an EX8200 Virtual Chassis:

```
user@switch> request system firmware upgrade fpc slot slot-number member member-id

Firmware upgrade initiated....
Please wait for ~2mins for upgrade to complete....
```

6. Confirm the loader software upgrade:

```
user@switch> show system firmware
```

Part	Type	Tag	Current version	Available version	Status
FPC 6	U-Boot	0	2.3.0		UPGRADED SUCCESSFULLY
FPC 7	U-Boot	0	2.3.0		OK
Routing Engine 0 RE BIOS		0	3.1.1		OK
Routing Engine 1		0	3.1.1		OK

The status is **UPGRADED SUCCESSFULLY** if the boot loader version update process is complete.

The status is **PROGRAMMING** if the boot loader version update process is still in progress.

Do not proceed to the next step until the **show system firmware** output confirms that the loader software upgrade is complete.

7. Restart the line card.

- To restart a line card on a standalone EX8200 switch:

```
user@switch> request chassis fpc restart slot slot-number
```

- To restart a line card on an EX8200 member switch in an EX8200 Virtual Chassis:

```
user@switch> request chassis fpc restart slot slot-number member member-id
```



NOTE: You can monitor the status of the line card restart by using the **show chassis fpc** command.

8. After the line card restart has completed, confirm the loader software version update:

```
user@switch> show chassis firmware
```

Part	Type	Tag	Current version	Available version	Status
FPC 6	U-Boot	0	3.5.0		OK
FPC 7	U-Boot	0	2.3.0		OK
Routing Engine 0	RE BIOS	0	3.1.1		OK
Routing Engine 1		0	3.1.1		OK

The current version has updated to **3.5.0**. You have upgraded the loader software for one bank of the line card.

- Repeat Steps 4 through 7 to upgrade the loader software on the other bank of the line card.



NOTE: A bank switchover occurs automatically as part of the line card restart. Repeating Steps 3 through 6 updates the loader software on the other bank.

- Repeat Steps 4 through 8 for all other line cards that require a line card loader version upgrade.

Related Documentation

- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)*
- Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure)*
- Troubleshooting an EX8200 Line Card's Failure to Power On*

Upgrading Junos OS with Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run an upgraded FreeBSD kernel instead of older versions of FreeBSD.

Before you begin:

- Verify that the upgrade applies to your router or switch model, as listed in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).
- Download the Junos OS package.
- Determine the upgrade path to follow.

The current Junos OS release determines the upgrade path to Junos OS with upgraded FreeBSD, as shown in [Table 21](#). Other upgrade paths might work, but they are not supported.

Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD

Current Router's Junos OS Release	Upgrade Path
12.3 or earlier	Upgrade to 13.3, or 14.2 first, then upgrade to 15.1 or later (multiple steps).

Table 21: Upgrade Path to Junos OS with the Upgraded FreeBSD (*continued*)

Current Router's Junos OS Release	Upgrade Path
13.3 or later	Use upgrade package to upgrade from the current Junos OS release to Junos OS with upgraded FreeBSD (single step).
15.1 or later	Use upgrade package to upgrade from the current Junos OS release to Junos OS with upgraded FreeBSD (single step).



NOTE: You can also downgrade from Junos OS Release 15.1 to an earlier release of Junos OS, as long as the path complies with the Junos OS policy of skipping at most two releases earlier.

- Understand that direct validation of running configuration does not work for upgrading to Junos OS with upgraded FreeBSD from Junos OS based on older versions of the FreeBSD kernel.

When upgrading or downgrading between Junos OS and Junos OS with upgraded FreeBSD, you might have to validate on a different host. It does not matter where that other host is, as long as you can reach it with NETCONF over SSH. See *Establishing an SSH Connection for a NETCONF Session*. The target system uses the network to contact the other host, run the validation and authentication, and return the result.

The upgrade process only preserves the following directories:

- `/config`
- `/etc/localtime`
- `/var/db`
- `/var/etc/master.passwd`
- `/var/etc/inetd.conf`
- `/var/etc/pam.conf`
- `/var/etc/resolv.conf`
- `/var/etc/syslog.conf`
- `/var/etc/localtime`
- `/var/etc/exports`
- `/var/etc/extensions.allow`
- `/var/preserve`
- `/var/tmp/baseline-config.conf`
- `/var/tmp/preinstall_boot_loader.conf`



NOTE: On EX2300 and EX3400 switches, the following directories are not applicable:

- /etc/localtime
- /var/etc/localtime
- /var/etc/exports
- /var/preserve
- /var/tmp/preinstall_boot_loader.conf

For specific installation procedures, see the following:

- [To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS on page 141](#)
- [To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release on page 144](#)
- [To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release on page 145](#)

To Install Junos OS with Upgraded FreeBSD Over a Plain Junos OS



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over a plain Junos OS:

1. Enter the **request system software add *package-name* no-validate** command from the operational mode in the CLI:



NOTE: The **no-copy** option is enabled by default.

Use the **no-validate** option with the **request system software add** command. If you leave out the **no-validate** option, the command uses the **validate** option by default, and direct validation of running configuration does not work for upgrading to Junos OS with upgraded FreeBSD from Junos OS based on older versions of the FreeBSD kernel.



NOTE: You can also use `reboot` option along with `request system software add` command, but it is not recommended to do this in a single step while upgrading from a FreeBSD 6.1 based Junos OS to FreeBSD 10 based Junos OS.



NOTE: To validate current configuration on an upgrade to Junos OS with upgraded FreeBSD from Junos OS, use the `request system software validate on (Junos OS with Upgraded FreeBSD)` command.

```
user@host>request system software add
/var/tmp/junos-install-mx-x86-32-15.1R1.9.tgz no-validate
Installing package '/var/tmp/junos-install-mx-x86-32-15.1R1.9.tgz' ...
Verified manifest signed by PackageProductionEc_2015
Verified manifest signed by PackageProductionRSA_2015
Verified contents.iso
Verified issu-indb.tgz
Verified junos-x86-32.tgz
Verified kernel
Verified metatags
Verified package.xml
Verified pkgtools.tgz
camcontrol: not found
camcontrol: not found
Verified manifest signed by PackageProductionEc_2015
Saving the config files ...
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install
Saving package file in
/var/sw/pkg/junos-install-x86-32-domestic-20150618.043753_builder_junos_151_r1.tgz
...
Saving state for rollback ...
```

The new Junos OS image is installed on the router.

2. Reboot the device to start the new software using the `request system reboot` command:

```
user@host> request system reboot
Reboot the system? [yes, no] (no) yes
```



NOTE: You must reboot the device to load the newly installed version of Junos OS on the device.

To abort the installation, do not reboot the device. Instead, finish the installation and then issue the `request system software delete package-name` command where package is, for example, `junos-install-mx-x86-32-15.1R1.9.tgz`. This is your last chance to stop the installation (not applicable on EX2300 and EX3400 platforms).

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The device then reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not route traffic.

3. Log in and issue the **show version** command to verify the version of the software installed.

```
user@host> show version
Hostname: host
Model: mx240
Junos: 15.1R1.9
JUNOS OS Kernel 32-bit [20150617.306001_builder_stable_10]
JUNOS OS runtime [20150617.306001_builder_stable_10]
JUNOS OS time zone information [20150617.306001_builder_stable_10]
JUNOS py base [20150618.043753_builder_junos_151_r1]
JUNOS OS crypto [20150617.306001_builder_stable_10]
JUNOS network stack and utilities [20150618.043753_builder_junos_151_r1]
JUNOS libs [20150618.043753_builder_junos_151_r1]
JUNOS runtime [20150618.043753_builder_junos_151_r1]
JUNOS platform support [20150618.043753_builder_junos_151_r1]
JUNOS modules [20150618.043753_builder_junos_151_r1]
JUNOS daemons [20150618.043753_builder_junos_151_r1]
JUNOS Voice Services Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services SSL [20150618.043753_builder_junos_151_r1]
JUNOS Services Stateful Firewall [20150618.043753_builder_junos_151_r1]
JUNOS Services RPM [20150618.043753_builder_junos_151_r1]
JUNOS Services PTSP Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services NAT [20150618.043753_builder_junos_151_r1]
JUNOS Services Mobile Subscriber Service Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Services MobileNext Software package
[20150618.043753_builder_junos_151_r1]
JUNOS Services LL-PDF Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Services Jflow Container package [20150618.043753_builder_junos_151_r1]
JUNOS Services IPSec [20150618.043753_builder_junos_151_r1]
JUNOS IDP Services [20150618.043753_builder_junos_151_r1]
JUNOS Services HTTP Content Management package
[20150618.043753_builder_junos_151_r1]
JUNOS Services Crypto [20150618.043753_builder_junos_151_r1]
JUNOS Services Captive Portal and Content Delivery Container package
[20150618.043753_builder_junos_151_r1]
JUNOS Border Gateway Function package [20150618.043753_builder_junos_151_r1]
JUNOS AppId Services [20150618.043753_builder_junos_151_r1]
JUNOS Services Application Level Gateways
[20150618.043753_builder_junos_151_r1]
JUNOS Services ACL Container package [20150618.043753_builder_junos_151_r1]
JUNOS Packet Forwarding Engine Support (MX/EX92XX Common)
[20150618.043753_builder_junos_151_r1]
JUNOS Packet Forwarding Engine Support (M/T Common)
[20150618.043753_builder_junos_151_r1]
JUNOS Online Documentation [20150618.043753_builder_junos_151_r1]
JUNOS FIPS mode utilities [20150618.043753_builder_junos_151_r1]
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of an Earlier Release



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over Junos OS with upgraded FreeBSD of an earlier release:

1. Enter the **request system software add *package-name* validate reboot** command from the operational mode in the CLI:



NOTE: The **no-copy** option is enabled by default.

Use the **validate** and **reboot** options with the **request system software add** command. The command uses the **validate** option by default. We encourage users to validate using the **validate** option when upgrading from Junos OS to Junos OS or from Junos OS with upgraded FreeBSD to Junos OS with upgraded FreeBSD.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.

The new Junos OS image is installed on the router.

2. Verify the installation of Junos OS with upgraded FreeBSD.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

To Install Junos OS with Upgraded FreeBSD Over Junos OS with Upgraded FreeBSD of a Later Release



NOTE: If you have important files in other directories, copy them from the router or switch to a secure location before upgrading the router or switch.



NOTE: The following procedure refers to routers, but it also applies to switches.

To install Junos OS with upgraded FreeBSD over Junos OS with upgraded FreeBSD of a later release:

1. Enter the **request system software add *package-name* validate reboot** command from the operational mode in the CLI:



NOTE: The **no-copy** option is enabled by default.

Use the **validate** and **reboot** options with the **request system software add** command. The command uses the **validate** option by default. We encourage users to validate using the **validate** option when upgrading from Junos OS to Junos OS or from Junos OS with upgraded FreeBSD to Junos OS with upgraded FreeBSD.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.

The new Junos OS image is installed on the router.

2. Verify the installation of Junos OS with upgraded FreeBSD.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Related Documentation

- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 316](#)

Understanding Junos OS Upgrades for SRX Series Devices

SRX Series devices are delivered with Junos OS preinstalled on them. When you power on a device, it starts (boots) up using its primary boot device. These devices also support

secondary boot devices, allowing you to back up your primary boot device and configuration.

As new features and software fixes become available, you must upgrade Junos OS to use them. Before an upgrade, we recommend that you back up your primary boot device.

Understanding Junos OS Upgrades

On a services gateway, you can configure the primary or secondary boot device with a snapshot of the current configuration, default factory configuration, or rescue configuration. You can also replicate the configuration for use on another device.

If the SRX Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the Junos OS package onto the corrupted internal media from a USB flash drive or TFTP server.

Junos OS Upgrade Methods on the SRX Series Devices

SRX Series devices that ship from the factory with Junos OS Release 10.0 or later are formatted with the dual-root partitioning scheme.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.

Existing SRX Series devices that are running Junos OS Release 9.6 or earlier use the single-root partitioning scheme. While upgrading these devices to Junos OS Release 10.0 or later, you can choose to format the storage media with dual-root partitioning (strongly recommended) or retain the existing single-root partitioning.

Certain Junos OS upgrade methods format the internal media before installation, whereas other methods do not. To install Junos OS Release 10.0 or later with the dual-root partitioning scheme, you must use an upgrade method that formats the internal media before installation.



NOTE: If you are upgrading to Junos OS Release 10.0 without transitioning to dual-root partitioning, use the conventional CLI and J-Web user interface installation methods.

These upgrade methods format the internal media before installation:

- Installation from the boot loader using a TFTP server
- Installation from the boot loader using a USB storage device
- Installation from the CLI using the **partition** option (available in Junos OS Release 10.0)
- Installation using the J-Web user interface

These upgrade methods retain the existing partitioning scheme:

- Installation using the CLI

- Installation using the J-Web user interface



WARNING: Upgrade methods that format the internal media before installation wipe out the existing contents of the media. Only the current configuration will be preserved. Any important data should be backed up before starting the process.



NOTE: Once the media has been formatted with the dual-root partitioning scheme, you can use conventional CLI or J-Web user interface installation methods, which retain the existing partitioning and contents of the media, for subsequent upgrades.

Related Documentation

- [Software Naming Convention for SRX Series Devices on page 10](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Preparing Your SRX Series Device for Junos OS Upgrades

Before you begin upgrading Junos OS on an SRX Series device, ensure the following:

- Obtain a Juniper Networks Web account and a valid support contract. You must have an account to download software upgrades. To obtain an account, complete the registration form at the Juniper Networks website:
<https://www.juniper.net/registration/Register.jsp>.
- Back up your primary boot device onto a secondary storage device.

Creating a backup has the following advantages:

- The device can boot from backup and come back online in case of failure or corruption of the primary boot device in the event of power failure during an upgrade.
- Your active configuration files and log files are retained.
- The device can recover from a known, stable environment in case of an unsuccessful upgrade.

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

Secondary Storage Devices Available on SRX Series Devices

You can use either the J-Web user interface or the CLI to back up the primary boot device on the secondary storage device.

[Table 22](#) lists the secondary storage devices available on an SRX Series devices.

Table 22: Secondary Storage Devices for SRX Series Devices

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX300, SRX320, SRX340, and SRX345 Services Gateways	1 GB
	SRX550M	2 GB
SSD Card	SRX1500	100 GB
Routing Engine (RE2) SSD card	SRX5000 line devices	120 GB

**NOTE:**

- During a successful upgrade, the upgrade package completely reinstalls the existing Junos OS. It retains configuration files, log files, and similar information from the previous version.
- After a successful upgrade, remember to back up the new current configuration to the secondary device.

Verifying Available Disk Space on SRX Series Devices

The amount of free disk space necessary to upgrade a device with a new version of Junos OS can vary from one release to another. Check the Junos OS software version you are installing to determine the free disk space requirements.

If the amount of free disk space on a device is insufficient for installing Junos OS, you might receive a warning similar to the following messages, that the /var filesystem is low on free disk space:

WARNING: The /var filesystem is low on free disk space.

WARNING: This package requires 1075136k free, but there is only 666502k available.

To determine the amount of free disk space on the device, issue the **show system storage detail** command. The command output displays statistics about the amount of free disk space in the device file systems.

A sample of the **show system storage detail** command output is shown below:

```
user> show system storage detail
```

Filesystem	1024-blocks	Used	Avail	Capacity	Mounted on
/dev/da0s2a	300196	154410	121772	56%	/
devfs	1	1	0	100%	/dev
/dev/md0	409000	409000	0	100%	/junos
/cf	300196	154410	121772	56%	/junos/cf
devfs	1	1	0	100%	/junos/dev/

procfs	4	4	0	100%	/proc
/dev/bo0s3e	25004	52	22952	0%	/config
/dev/bo0s3f	350628	178450	144128	55%	/cf/var
/dev/md1	171860	16804	141308	11%	/mfs
/cf/var/jail	350628	178450	144128	55%	/jail/var
/cf/var/log	350628	178450	144128	55%	/jail/var/log
devfs	1	1	0	100%	/jail/dev
/dev/md2	40172	4	36956	0%	/mfs/var/run/utm
/dev/md3	1884	138	1596	8%	/jail/mfs

Cleaning Up the System File Storage Space

When the system file storage space on the device is full, rebooting the device does not solve the problem. The following error message is displayed during a typical operation on the device after the file storage space is full.

```
user@host% cli
user@host> configure/var: write failed, filesystem is full
```

You can clean up the file storage on the device by deleting system files using the **request system storage cleanup** command as shown in following procedure:

1. Request to delete system files on the device.

```
user@host> request system storage cleanup
```

The list of files to be deleted is displayed.

List of files to delete:

Size	Date	Name
11B	Oct 28 23:40	/var/jail/tmp/alarmd.ts
92.4K	Jan 11 17:12	/var/log/chassisd.0.gz
92.4K	Jan 11 06:06	/var/log/chassisd.1.gz
92.5K	Jan 10 19:00	/var/log/chassisd.2.gz
92.5K	Jan 10 07:53	/var/log/chassisd.3.gz
92.2K	Jan 10 15:00	/var/log/hostlogs/auth.log.1.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.2.gz
92.1K	Jan 4 17:30	/var/log/hostlogs/auth.log.3.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.4.gz
79.0K	Jan 12 01:59	/var/log/hostlogs/daemon.log.1.gz
78.8K	Jan 11 23:15	/var/log/hostlogs/daemon.log.2.gz
78.7K	Jan 11 20:30	/var/log/hostlogs/daemon.log.3.gz
79.1K	Jan 11 17:44	/var/log/hostlogs/daemon.log.4.gz
59.1K	Jan 11 21:59	/var/log/hostlogs/debug.1.gz
59.2K	Jan 11 17:44	/var/log/hostlogs/debug.2.gz
59.2K	Jan 11 13:29	/var/log/hostlogs/debug.3.gz
59.3K	Jan 11 09:14	/var/log/hostlogs/debug.4.gz
186.6K	Oct 20 16:31	/var/log/hostlogs/kern.log.1.gz
238.3K	Jan 11 23:15	/var/log/hostlogs/lcmd.log.1.gz
238.4K	Jan 11 17:30	/var/log/hostlogs/lcmd.log.2.gz
238.6K	Jan 11 11:45	/var/log/hostlogs/lcmd.log.3.gz
238.5K	Jan 11 06:00	/var/log/hostlogs/lcmd.log.4.gz
372.5K	Jan 11 17:00	/var/log/hostlogs/syslog.1.gz
372.5K	Jan 11 04:45	/var/log/hostlogs/syslog.2.gz
371.9K	Jan 10 16:30	/var/log/hostlogs/syslog.3.gz
372.7K	Jan 10 04:15	/var/log/hostlogs/syslog.4.gz
10.1K	Jan 12 02:03	/var/log/messages.0.gz
55.1K	Jan 6 21:25	/var/log/messages.1.gz
81.5K	Dec 1 21:30	/var/log/messages.2.gz

Delete these files ? [yes,no] (no)

2. Enter the option **yes** to proceed with deleting of the files.

Downloading Software Packages from Juniper Networks

To download Junos OS upgrades from Juniper Networks:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks webpage. Depending on your location, select the Canada and U.S. version (domestic) or the Worldwide version (ww):
 - <https://www.juniper.net/support/downloads/junos.html>
 - <https://www.juniper.net/support/downloads/junos.html>
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by your Juniper Networks representative.
3. Select the appropriate software image for your platform.
4. Download Junos OS to a local host or to an internal software distribution site.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server on page 152](#)

Example: Installing Junos OS Upgrade Packages on SRX Series Devices

This example shows how to install Junos OS upgrades on SRX Series devices.

- [Requirements on page 150](#)
- [Overview on page 151](#)
- [Configuration on page 151](#)
- [Verification on page 152](#)

Requirements

Before you begin:

- Verify the available space on the internal media. See “[Preparing Your SRX Series Device for Junos OS Upgrades](#)” on [page 147](#) and the *Junos OS Release Notes*
- Download the software package. See “[Downloading Software Packages from Juniper Networks](#)” on [page 150](#).
- Copy the software package to the device if you are installing the software package from a local directory on the device. We recommend that you copy it to the `/var/tmp` directory.

Overview

By default, the **request system software add *package-name*** command uses the **validate** option to validate the software package against the current configuration as a prerequisite to adding the software package. This validation ensures that the device can reboot successfully after the software package is installed. This is the default behavior when you are adding a software package.

In this example, add the software package `junos-srxsme-10.0R2-domestic.tgz` (for SRX Series devices) with the following options:

- **no-copy** option to install the software package but do not save the copies of package files. You should include this option if you do not have enough space on the internal media to perform an upgrade that keeps a copy of the package on the device.
- **no-validate** option to bypass the compatibility check with the current configuration before installation starts.
- **reboot** option to reboots the device after installation is completed.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz
no-copy no-validate reboot
```

GUI Step-by-Step Procedure

To install Junos OS upgrades on SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Upload Package**.
2. On the Upload Package page, specify the software package to upload. Click **Browse** to navigate to the software package location and select `junos-srxsme-10.0R2-domestic.tgz`.
3. Select the **Reboot If Required** check box to set the device to reboot automatically when the upgrade is complete.
4. Select the **Do not save backup** check box to bypass saving the backup copy of the current Junos OS package (SRX Series).
5. Click **Upload Package**. The software is activated after the device has rebooted.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

From operational mode, install the new package on the device with the no-copy and no-validate options, and format and re-partition the media before installation, and reboot the device after installation is completed.

To install Junos OS upgrades on SRX Series devices:

1. From operational mode, install the new package on the device

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz  
no-copy no-validate
```

2. Reboot the device.

```
user@host> request system reboot
```

When the reboot is complete, the device displays the login prompt.

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Junos OS Upgrade Installation on page 152](#)

Verifying the Junos OS Upgrade Installation

Purpose Verify that the Junos OS upgrade was installed.

Action From operational mode, enter the **show system** command.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 66](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Downloading Software Packages from Juniper Networks on page 150](#)
- [Configure Administration User Accounts on page 174](#)

Installing Junos OS Upgrade Packages on SRX Series Devices from a Remote Server

You can use the J-Web user interface to install Junos OS packages that are retrieved with FTP or HTTP from the specified location.



NOTE: This procedure applies only to upgrading from one Junos OS release to another.

Before installing the Junos OS upgrade:

- Verify the available space on the internal media. See “[Preparing Your SRX Series Device for Junos OS Upgrades](#)” on page 147 and the *Junos OS Release Notes*
- Download the software package. See “[Downloading Software Packages from Juniper Networks](#)” on page 150.

To install Junos OS upgrades from a remote server:

1. In the J-Web user interface, select **Maintain>Software>Install Package**.
2. On the Install Remote page, enter the required information in the fields described in [Table 10](#).

Table 23: Install Package Summary

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and Junos OS package name.	Type the full address of the Junos OS package location on the FTP or HTTP server—one of the following: <i>ftp://hostname/pathname/package-name</i> <i>http://hostname/pathname/package-name</i>
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	Specifies that the device is automatically rebooted when the upgrade is complete.	Check the box if you want the device to reboot automatically when the upgrade is complete.
Do not save backup (SRX Series devices)	Specifies that the backup copy of the current Junos OS package is not saved.	Check the box if you want to save the backup copy of the Junos OS package.
Format and re-partition the media before installation (SRX Series devices)	Specifies that the storage media is formatted and new partitions are created.	Check the box if you want to format the internal media with dual-root partitioning.

3. Click **Fetch and Install Package**. Junos OS is activated after the device reboots.

- Related Documentation**
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
 - [Configure Administration User Accounts on page 174](#)

Understanding BIOS Upgrades on SRX Series Devices

Understanding Manual BIOS Upgrade Using the Junos CLI

For these SRX Series devices, the BIOS consists of a U-boot and the Junos loader. The SRX300, and SRX320 Service Gateways also include a U-shell binary as part of the BIOS. Additionally, on SRX300, SRX320, SRX340, and SRX345 Service Gateways, a backup BIOS is supported which includes a backup copy of the U-boot in addition to the active copy from which the system generally boots up.

Table 24 Lists the CLI commands used for manual BIOS upgrade.

Table 24: CLI Commands for Manual BIOS Upgrade

Active BIOS	Backup BIOS
<code>request system firmware upgrade re bios</code>	<code>request system firmware upgrade re bios backup</code>

BIOS upgrade procedure:

1. **Install the jloader-srxsme package.**

1. Copy the jloader-srxsme signed package to the device.



NOTE: The version of the jloader-srxsme package you install must match the version of Junos OS.

2. Install the package using the `request system software add <path to jloader-srxsme package> no-copy no-validate` command.



NOTE: Installing the jloader-srxsme package places the necessary images under directory/boot.

2. Verify that the required images for upgrade are installed. Use the `show system firmware` to verify that the correct BIOS image version is available for upgrade.
3. Upgrade the BIOS (Active and backup) image.

Active BIOS:

1. Initiate the upgrade using the `request system firmware upgrade re bios` command.
2. Monitor the upgrade status using the `show system firmware` command.



NOTE: The device must be rebooted for the upgraded active BIOS to take effect.

Backup BIOS:

1. Initiate the upgrade using the **request system firmware upgrade re bios backup** command.
2. Monitor the upgrade status using the **show system firmware** command.

Understanding Auto BIOS Upgrade Methods on SRX Series Devices

The BIOS version listed in the **bios-autoupgrade.conf** file is the minimum supported version. If the current device has a BIOS version earlier than the minimum compatible version, then the auto BIOS upgrade feature upgrades the BIOS automatically to the latest version.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI (using the **request system software add no-copy no-validate software-image**). In this case, only the active BIOS is upgraded.
- During loader installation using TFTP or USB (using the **install tftp:///software-image** command). In this case, only the active BIOS is upgraded.
- During system boot-up. In this case, both the active BIOS and the backup BIOS are upgraded.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 70](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 72](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 155](#)

Disabling Auto BIOS Upgrade on SRX Series Devices

The auto BIOS upgrade feature is enabled by default. You can disable the feature using the CLI in operational mode.

To disable the automatic upgrade of the BIOS on an SRX Series device, set the **chassis routing-engine bios** command.

```
user@host> set chassis routing-engine bios no-auto-upgrade
```



NOTE: The command disables automatic upgrade of the BIOS only during Junos OS upgrade or system boot-up. It does not disable automatic BIOS upgrade during loader installation.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 154](#)

Example: Downgrading Junos OS on SRX Series Devices

This example shows how to downgrade Junos OS on the SRX Series devices.

- [Requirements on page 156](#)
- [Overview on page 156](#)
- [Configuration on page 156](#)
- [Verification on page 158](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

When you upgrade your software, the device creates a backup image of the software that was previously installed in addition to installing the requested software upgrade.

To downgrade the software, you can revert to the previous image using the backup image. You can use this method to downgrade to only the software release that was installed on the device before the current release. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release. This example returns software to the previous Junos OS version.



NOTE: This procedure applies only to downgrading from one Junos OS software release to another or from one Junos OS services release to another.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host>
request system software rollback
```

request system reboot**GUI Step-by-Step Procedure**

To downgrade Junos OS on SRX Series devices:

1. In the J-Web user interface, select **Maintain>Software>Downgrade**. The image of the previous version (if any) appears on this page.



NOTE: After you perform this operation, you cannot undo it.

2. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.
3. Click **Maintain>Reboot** from the J-Web user interface to reboot the device.



NOTE: To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To downgrade Junos OS on SRX Series devices:

1. From operational mode, return to the previous Junos OS version.

```
user@host> request system software rollback
```

2. Reboot the device.

```
user@host> request system reboot
```

The device is now running the previous version of Junos OS. To downgrade to an earlier version, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Junos OS Downgrade Installation on page 158](#)

Verifying the Junos OS Downgrade Installation

Purpose Verify that the Junos OS downgrade was installed.

Action From operational mode, enter the **show system** command.

- Related Documentation**
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
 - [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
 - [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
 - [Restarting and Halting SRX Series Devices on page 213](#)

CHAPTER 9

Booting a Device Using a System Snapshot

- [Understanding System Snapshot on EX Series Switches on page 159](#)
- [Creating a Snapshot and Using It to Boot an EX Series Switch on page 160](#)
- [Verifying That a System Snapshot Was Created on an EX Series Switch on page 161](#)
- [Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive on page 162](#)

Understanding System Snapshot on EX Series Switches

You can create copies of the software running a Juniper Networks EX Series Ethernet Switch using the system snapshot feature. The system snapshot feature takes a “snapshot” of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

The switch can boot from either internal flash media or external (USB) flash media. The contents of the snapshot vary depending on whether you create the snapshot on the media that the switch booted from or on the media that it did not boot from:

Snapshots are particularly useful for moving files onto USB flash drives. You cannot use the **copy** command or any other file-moving technique to move files from an internal memory source to USB memory on the switch.

- If you create the snapshot on the media that the switch did not boot from, the following partitions on the boot media are included in the snapshot: **root**, **altroot**, **var**, **var/tmp**, **config**.

The **root** partition is the primary boot partition, and the **altroot** partition is the backup boot partition.

- If you create the snapshot on the media that the switch booted from, the root partition that the switch booted from is copied to the alternate root partition. The **var**, **var/tmp**, and **config** partitions are not copied as part of the snapshot because they already exist on the boot media.

The system snapshot feature has the following limitations:

- You cannot use snapshots to move files to any destination outside the switch other than an installed external USB flash drive or switches that are members of the same Virtual Chassis as the switch on which you created the snapshot..
- Snapshot commands, like all commands executed on a Virtual Chassis, are executed on the local member switch. If different member switches request the snapshot, the snapshot command is pushed to the Virtual Chassis member creating the snapshot and is executed on that member, and the output is then returned to the switch that initiated the process. For instance, if the command to create an external snapshot on member 3 is entered on member 1, the snapshot of internal memory on member 3 is taken on external memory on member 3. The output of the process is seen on member 1. No files move between the switches.

**Related
Documentation**

- [Understanding Software Installation on EX Series Switches on page 44](#)
- [Creating a Snapshot and Using It to Boot an EX Series Switch on page 160](#)

Creating a Snapshot and Using It to Boot an EX Series Switch

The system snapshot feature takes a “snapshot” of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

This topic includes the following tasks:

- [Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch on page 160](#)

Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch

You can create a snapshot on USB flash memory after a switch is booted by using files stored in internal memory.

Ensure that you have the following tools and parts available before creating a snapshot on a USB flash drive:

- A USB flash drive that meets the switch USB port specifications. See *USB Port Specifications for an EX Series Switch*.

To create a snapshot on USB flash memory and use it to boot the switch:

1. Place the snapshot into USB flash memory:

```
user@switch> request system snapshot partition media usb
```
2. (Optional) Perform this step if you want to boot the switch now using the snapshot stored on the USB flash drive.

```
user@switch> request system reboot media usb
```

**Related
Documentation**

- [Verifying That a System Snapshot Was Created on an EX Series Switch on page 161](#)
- [Understanding System Snapshot on EX Series Switches on page 159](#)

Verifying That a System Snapshot Was Created on an EX Series Switch

Purpose Verify that a system snapshot was created with the proper files on an EX Series switch.

Action View the snapshot:

```
user@switch> show system snapshot media external
Information for snapshot on      external (/dev/da1s1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on      external (/dev/da1s2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

Meaning The output shows the date and time when the snapshot was created and the packages that are part of the snapshot. Check to see that the date and time match the time when you created the snapshot.

You can compare the output of this command to the output of the **show system software** command to ensure that the snapshot contains the same packages as the software currently running the switch.

Related Documentation

- [Creating a Snapshot and Using It to Boot an EX Series Switch on page 160](#)

Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive

There are two methods of getting Junos OS stored on a USB flash drive before using the software to boot the switch. You can pre-install the software onto the USB flash drive before inserting the USB flash drive into the USB port, or you can use the system snapshot feature to copy files from internal switch memory to the USB flash drive.

To move files into USB flash memory by using a system snapshot and use those files to boot the switch, see [“Creating a Snapshot and Using It to Boot an EX Series Switch” on page 160](#). We recommend that you use this method to boot the switch from a USB flash drive if your switch is running properly.

If you need to pre-install the software onto the USB flash drive, you can use the method described in this topic. Pre-installing Junos OS onto a USB flash drive to boot the switch can be done at any time and is particularly useful when the switch boots to the loader prompt because the switch cannot locate the Junos OS in internal flash memory.

Ensure that you have the following tools and parts available to boot the switch from a USB flash drive:

- A USB flash drive that meets the EX Series switch USB port specifications. See *USB Port Specifications for an EX Series Switch*.
- A computer or other device that you can use to download the software package from the Internet and copy it to the USB flash drive.

To download a Junos OS package onto a USB flash drive before inserting the USB flash drive:

1. Download the Junos OS package that you want to place onto the EX Series switch from the Internet onto the USB flash drive by using your computer or other device. See [“Downloading Software Packages from Juniper Networks” on page 51](#).
2. Remove the USB flash drive from the computer or other device.
3. Insert the USB flash drive into the USB port on the switch.
4. This step can be performed only when the prompt for the loader script (**loader>**) is displayed. The loader script starts when the Junos OS loads but the CLI is not working for any reason or if the switch has no software installed.

Install the software package onto the switch:

```
loader> install source
```

where **source** represents the name and location of the Junos OS package on the USB flash drive. The Junos OS package on a flash drive is commonly stored in the root drive as the only file—for example, **file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**.

Related Documentation

- [Installing Software on an EX Series Switch with a Single Routing Engine \(CLI Procedure\)](#)
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)

- See *EX2200 Switches Hardware Overview* for USB port location.
- See *Rear Panel of an EX3200 Switch* for USB port location.
- See *Rear Panel of an EX3300 Switch* for USB port location.
- See *Rear Panel of an EX4200 Switch* for USB port location.
- See *EX4300 Switches Hardware Overview* for USB port location.
- See *Front Panel of an EX4500 Switch* for USB port location.
- See *EX4550 Switches Hardware Overview* for USB port location.
- See *Switch Fabric and Routing Engine (SRE) Module in an EX6200 Switch* for USB port location.
- See *Switch Fabric and Routing Engine (SRE) Module in an EX8208 Switch* for USB port location.
- See *Routing Engine (RE) Module in an EX8216 Switch* for USB port location.

CHAPTER 10

Performing a Recovery Installation

- [Creating an Emergency Boot Device on page 165](#)
- [Configuring Boot Devices for SRX Series Devices on page 166](#)
- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 169](#)
- [Performing a Recovery Installation on page 172](#)
- [Creating a New Configuration on a Single Routing Engine on page 173](#)
- [Creating a New Configuration with Redundant Routing Engines on page 177](#)
- [Saving a Rescue Configuration File on page 183](#)
- [Restoring a Saved Configuration on page 184](#)
- [Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 185](#)
- [Reverting to the Rescue Configuration on page 186](#)

Creating an Emergency Boot Device

If the device's Junos OS software is damaged in some way that prevents Junos OS software from loading completely, you can use the emergency boot device to revive the device. The emergency boot device repartitions the primary disk and reloads a fresh installation of Junos OS software.

The procedures outlined in this section discuss how to create an emergency boot device for any ACX Series, M Series, MX Series, T Series, TX Matrix, and TX Matrix Plus router.

To create an emergency boot device:

1. Use FTP to copy the installation media into the router's **/var/tmp** directory.
2. Insert the PC Card into the external PC Card slot or USB storage device into the USB port.
3. In the UNIX shell, navigate to the **/var/tmp** directory:

```
start shell
cd /var/tmp
```
4. Log in as **su**:

```
su [enter]
```

```
password: [enter SU password]
```

5. Issue the following commands:

```
dd if=/dev/zero of=/dev/externalDrive count=20
dd if=installMedia of=/dev/externalDrive bs=64k
```

where:

- **externalDrive**—Refers to the removable media name of the emergency boot device. For example, the removable media name for an emergency boot device on the M120 router is *da0* for both Routing Engines. For the names of the storage media, see [“Routing Engines and Storage Media Names \(ACX Series, M Series, MX Series, PTX Series, T Series, TX Matrix, TX Matrix Plus, and JCS 1200 Routers\)” on page 32](#).
- **installMedia**—Refers to the installation media downloaded into the */var/tmp* directory. For example, **install-media-9.0R2.10-domestic.tgz**.

The following code example can be used to create an emergency boot device using a PC Card on an M20 router:

```
dd if=/dev/zero of=/dev/ad3 count=20
dd if=install-media-9.0R2.10-domestic.tgz of=/dev/ad3 bs=64k
```

The following code example can be used to create an emergency boot device using a USB storage device on an M120 router or a TX Matrix Plus router:

```
dd if=/dev/zero of=/dev/da0 count=20
dd if=install-media-9.0R2.10-domestic.tgz of=/dev/da0 bs=64k
```

6. Log out as **su**:

```
exit
```

Configuring Boot Devices for SRX Series Devices

This topic includes the following sections:

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)

Example: Creating a Snapshot and Using It to Boot an SRX Series Device

This example shows how to configure a boot device.

- [Requirements on page 166](#)
- [Overview on page 167](#)
- [Configuration on page 167](#)
- [Verification on page 168](#)

Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 1 GB. See [“Preparing Your SRX Series Device for Junos OS Upgrades” on page 147](#).

Overview

You can configure a boot device to replace the primary boot device on your SRX Series device or to act as a backup boot device. Use either the J-Web user interface or the CLI to take a snapshot of the configuration currently running on the device, or of the original factory configuration and a rescue configuration, and save it to an alternate medium.



NOTE: For media redundancy, we recommend that you keep a secondary storage medium attached to the SRX Series device and updated at all times.

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary internal media from the TFTP installation.

You can also configure a boot device to store snapshots of software failures for use in troubleshooting.



NOTE: You cannot copy software to the active boot device.



NOTE: After a boot device is created with the default factory configuration, it can operate only in an internal media slot.

This example configures a boot device to back up the currently running and active file system partitions by rebooting from internal media and including only files shipped from the factory.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host> request system snapshot partition media internal factory
```

GUI Step-by-Step Procedure

To configure a boot device:

1. In the J-Web user interface, select **Maintain>Snapshot**.
2. On the Snapshot page, specify the boot device to copy the snapshot to. From the Target Media list, select the **internal** boot device.
3. Select the Factory check box to copy only default files that were loaded on the internal media when it was shipped from the factory, plus the rescue configuration if one has been set.

4. Select the Partition check box to partition the medium that you are copying the snapshot to. This process is usually necessary for boot devices that do not already have software installed on them.
5. Click **Snapshot**.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To configure a boot device:

From operational mode, create a boot device from the internal media including only files shipped from the factory that will be used to back up the currently running and active file system partitions.

```
user@host> request system snapshot partition media internal factory
```

Results From configuration mode, confirm your configuration by entering the **show system snapshot media internal** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host> show system snapshot media internal
```

```
Information for snapshot on      internal (/dev/ad0s1a) (backup)
Creation date: Oct 9 13:30:06 2009
JUNOS version on snapshot:
  junos : 10.0B3.10-domestic
Information for snapshot on      internal (/dev/ad0s2a) (primary)
Creation date: Jan 6 15:45:35 2010
JUNOS version on snapshot:
  junos : 10.2-20091229.2-domestic
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Snapshot Information on page 168](#)

Verifying the Snapshot Information

Purpose Verify that the snapshot information for both root partitions on SRX Series devices were configured.

Action From operational mode, enter the **show system snapshot media** command.

The command output displays the snapshot creation time and Junos OS Release version on a media for both the primary and backup roots.



NOTE: With the dual-root partitioning scheme, performing a snapshot to a USB storage device that is less than 1 GB is not supported.



NOTE: You can use the `show system snapshot media internal` command to determine the partitioning scheme present on the internal media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.



NOTE: Any removable media that has been formatted with dual-root partitioning will not be recognized correctly by the `show system snapshot CLI` command on systems that have single-root partitioning. Intermixing dual-root and single-root formatted media on the same system is strongly discouraged.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 147](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 145](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices

This topic includes the following sections:

- [Overview on page 169](#)
- [How Autorecovery Works on page 170](#)
- [How to Use Autorecovery on page 170](#)
- [Data That Is Backed Up in an Autorecovery on page 170](#)
- [Troubleshooting Alarms on page 171](#)
- [Considerations on page 171](#)

Overview

The autorecovery feature is supported on dual-partitioned SRX Series devices. With this feature, information on disk partitioning, configuration, and licenses is recovered automatically in the event it becomes corrupted.

Autorecovery provides the following functions:

- Detect corruption in disk partitioning during system bootup and attempt to recover partitions automatically

- Detect corruption in the Junos OS rescue configuration during system bootup and attempt to recover the rescue configuration automatically
- Detect corruption in Junos OS licenses during system bootup and attempt to recover licenses automatically

How Autorecovery Works

The feature works in the following ways:

- The feature provides the **request system autorecovery state save** command, which backs up important data such as disk partitioning information, licenses, and Junos OS rescue configuration.
- Once the backup copies are saved, they are used to check the integrity of the working copies of the data on every bootup.
- The working copies are automatically recovered if any corruption is detected.

How to Use Autorecovery

You use autorecovery in the following ways:

- Prepare the router for deployment with the necessary licenses and configuration.
- After you finalize the state, execute the **request system autorecovery state save** command to back up the state.
- After you save the state, integrity check and recovery actions (if any) occur automatically on every bootup.
- If subsequent maintenance activities change the state of the router by adding licenses or updating the configuration, you need to execute the **request system autorecovery state save** command again to update the saved state.
- Execute the **show system autorecovery state** command any time to view the status of the saved information and the integrity check status of each saved item.
- Execute the **request system autorecovery state clear** command to delete all backed up data and disable autorecovery, if required.

Data That Is Backed Up in an Autorecovery

The following data is backed up during the autorecovery process:

- Rescue configuration (regenerated from the current configuration)
- License keys
- BSD labels (disk-partitioning information)

Data is backed up only when you execute the **request system autorecovery state save** command. Disk-partitioning information is backed up automatically from factory defaults (for new systems), on installation from the boot loader, and on snapshot creation.

Troubleshooting Alarms

Table 25 lists types of autorecovery alarms, descriptions, and required actions.

Table 25: Autorecovery Alarms

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: <ul style="list-style-type: none"> Unsaved data needs to be saved, or saved data contains problems and another save is required. 	<ul style="list-style-type: none"> Ensure that the system has all required licenses and configuration. Execute the request system autorecovery state save command.
Autorecovery has recovered corrupted information	Minor	This alarm indicates: <ul style="list-style-type: none"> Boot time integrity check failed for certain items; however, the items have been recovered successfully. 	<ul style="list-style-type: none"> No action is required. Alarm will be cleared on next bootstrap.
Autorecovery was unable to recover data completely	Major	This alarm indicates: <ul style="list-style-type: none"> Boot time integrity check failed for certain items, which could not be recovered successfully. 	<ul style="list-style-type: none"> The system might be experiencing a fatal malfunction.

Considerations

- Devices must have dual-root partitioning for autorecovery to work.
- The **request system configuration rescue save** command regenerates the rescue configuration from the current Junos OS configuration and then saves it. Therefore, executing the **save** command overwrites any existing rescue configuration.
- In general, the saved contents of the rescue configuration are not updated automatically. If you add licenses, you should execute the **request system autorecovery state save** command again.



NOTE: The rescue configuration is backed up. If /config is corrupted, the system boots from the rescue configuration.

Related Documentation

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 156](#)

Performing a Recovery Installation

If the device's software is corrupted or otherwise damaged, you may need to perform a recovery installation, using the emergency boot device to restore the default factory installation. Once you have recovered the software you will need to restore the router or switch's configuration. You can either create a new configuration as you did when the device was shipped from the factory, or if you saved the device's previous configuration, you can simply restore that file to the system.

Depending on the situation, you should try to perform the following steps before you perform the recovery installation:

1. Ensure you have an emergency recovery disk to use during the installation. When the router or switch is first shipped, an emergency recovery disk is provided with it. For instructions on creating an emergency boot device, see ["Creating an Emergency Boot Device" on page 165](#)
2. Copy the existing configuration in the file `/config/juniper.conf.gz` from the device to a remote system. For extra safety, you can also copy the backup configurations (the files named `/config/juniper.conf.n`, where *n* is a number from 0 through 9).



WARNING: The recovery installation process completely overwrites the entire contents of the fixed storage media.

3. Copy any other stored files to a remote system as desired.

To reinstall Junos OS:

1. Insert the removable media emergency boot device into the device.



NOTE: You can store a configuration on installation media such as a PC Card or USB stick.

2. Reboot the device.

If the CLI is still active, issue the **request system reboot** command from command mode to reboot the device.

If the CLI is not working, manually power off the device using the main power switch, wait 10 seconds, and then power the device back on.

3. When the software prompts you with the following question, type **y**:

WARNING: The installation will erase the contents of your disk. Do you wish to continue (y/n)? **y**

The device copies the software from the removable media emergency boot device onto your system, occasionally displaying status messages. Copying the software can take up to 45 minutes depending on the device. When the process is complete, the router boots into Amnesiac state and the login prompt is displayed.

4. Remove the removable media emergency boot device.
5. Login as root on the device's console port and issue the **request system reboot** command from command mode to reboot the device.

The device reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt.

6. Create a new configuration as you did when the device was shipped from the factory, or restore a previously saved configuration file to the system. For more information, see [“Creating a New Configuration on a Single Routing Engine” on page 173](#), [“Creating a New Configuration with Redundant Routing Engines” on page 177](#), and [“Restoring a Saved Configuration” on page 184](#).

Creating a New Configuration on a Single Routing Engine

To create a new base configuration on a single Routing Engine:

- [Log In to the Router Console on page 173](#)
- [Configure Administration User Accounts on page 174](#)
- [Add the Management Console to the Network on page 174](#)
- [Commit Changes on page 175](#)

Log In to the Router Console

To log in to the device's console interface and open the CLI in configuration mode:

1. Verify the device is powered on.
2. Log in through the console port as root.

```
Amnesiac <tttyd0>
```

```
login: root
```



NOTE: From the factory, the root administration user account is not associated with a password. However, you must add a password to the root administration account before you can successfully commit a configuration.

3. Start the CLI, which initially opens in operational mode. Note the command prompt ends with > in the CLI operational mode.

```
root@% cli
root>
```

4. Enter the CLI configuration mode. Note the command prompt ends with # in the CLI configuration mode.

```
root> configure
[edit]
root#
```

Configure Administration User Accounts

Set the root administration user account password. You also need to set up one or more administration user accounts. These administration user accounts are used to log in to the device through the management console. To configure administration user accounts:

1. Add a password to the root (superuser) administration user account.

```
[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

2. Create a management console user account.

```
[edit]
root# set system login user user-name authentication plain-text-password
New Password: password
Retype new password: password
```

3. Set the user account class to **super-user**.

```
[edit]
root# set system login user user-name class super-user
```

Add the Management Console to the Network

To add the management console to the network:

1. Specify the device hostname.



NOTE: The hostname specified in the device configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, this hostname appears on the command line prompt when the user is logged in to the CLI:

```
user-name@host-name>
```

```
[edit]
root# set system host-name host-name
```

2. Configure the IP address of the DNS server.

```
[edit]
root# set system name-server address
```

3. Configure the router or switch domain name.

```
[edit]
root# set system domain-name domain-name
```

4. Configure the IP address and prefix length for the router or switch Ethernet interface.

- For all devices *except* the TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

```
[edit]
```

```
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only, and PTX Series Packet Transport Routers:

```
[edit]
```

```
root@# set interfaces em0 unit 0 family inet address address/prefix-length
```

To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

- For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

```
[edit]
```

```
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- Configure the IP address of a backup router. The backup router is used while the local router is booting and if the routing process fails to start. Once the routing process starts, the backup router address is removed from the local routing and forwarding tables. For more information about the backup router, see the *Getting Started Guide for Routing Devices*.

```
[edit]
```

```
root# set system backup-router address
```

- (Optional) Configure the static routes to remote subnets with access to the management port. Access to the management port is limited to the local subnet. To access the management port from a remote subnet, you need to add a static route to that subnet within the routing table.

```
[edit]
```

```
root# set routing-options static route remote-subnet next-hop destination-IP retain no-readvertise
```

- Configure telnet service at the **[edit system services]** hierarchy level.

```
[edit]
```

```
root# set system services telnet
```

Commit Changes

Now that you have completed your changes to the configuration file, commit the configuration changes.

- Before committing the configuration, you can review your changes to the configuration with the **show** command.

```
root# show
## Last changed: 2008-08-27 22:30:42 UTC
version 9.3B1.5;
system {
  host-name tp8;
  domain-name subnet.device1.example.com;
  backup-router 192.168.71.254;
  root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
  }
  name-server {
    192.168.5.68;
```

```
        172.17.28.101;
    }
    login {
        user PE1 {
            class super-user;
            authentication {
                encrypted-password "$ABC123"; ## SECRET-DATA
            }
        }
    }
    services {
        telnet;
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.69.205/21;
            }
        }
    }
}
routing-options {
    static {
        route 172.16.0.0/12 {
            next-hop 192.168.71.254;
            retain;
            no-readvertise;
        }
        route 192.168.0.0/16 {
            next-hop 192.168.71.254;
            retain;
            no-readvertise;
        }
    }
}
```

On a TX Matrix Plus router and PTX Series Packet Transport Routers, the management Ethernet interface is **em0** and not **fxp0**. Therefore, when you issue the **show** command in the configuration mode, the configuration statements would be:

```
[edit]
root@ show
system {
    host-name hostname;
    domain-name domain.name;
    backup-router address;
    root-authentication {
```



```

        (encrypted-password "password" | public-key);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
    name-server {
        address;
    }
    interfaces {
        em0 {
            unit 0 {
                family inet {
                    address address ;
                }
            }
        }
    }
}

```

2. Commit the configuration.

```

[edit]
root# commit
commit complete

```



NOTE: If you receive an error message after you issue the `commit` statement, you can review the configuration using the `show` command to find the errors in your configuration. You can delete incorrect entries using the `delete` command. For example, to delete a hostname from the configuration, issue the following statement:

```

[edit]
root# delete system host-name host-name

```

3. Exit configuration mode.

```

[edit]
root# exit
Exiting configuration mode

root>

```

Creating a New Configuration with Redundant Routing Engines

To create a new base configuration on a router with redundant Routing Engines:

- [Configure Administration User Accounts on page 178](#)
- [Set Up Routing Engine Configuration Groups on page 178](#)
- [Complete the Management Console Configuration on page 180](#)
- [Commit and Synchronize Changes on page 181](#)

Configure Administration User Accounts

Set the root administration user account password. You also need to set up one or more administration user accounts. These administration user accounts are used to log in to the device through the management console. To configure administration user accounts:

1. Add a password to the root (superuser) administration user account.

```
[edit]
root# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

2. Create a management console user account.

```
[edit]
root# set system login user user-name authentication plain-text-password
New Password: password
Retype new password: password
```

3. Set the user account class to **super-user**.

```
[edit]
root# set system login user user-name class super-user
```

Set Up Routing Engine Configuration Groups

In a router with two Routing Engines, one configuration should be shared between both Routing Engines. This ensures that both Routing Engine configurations are identical. Within this configuration, create two Routing Engine groups, one for each Routing Engine. Within these groups, you specify the Routing Engine–specific parameters.

For more information about creating configuration groups, see *CLI User Guide*.

For more information about the initial configuration for redundant Routing Engine systems and the re0 group, see *Junos OS High Availability Library for Routing Devices*.

1. Create the configuration group **re0**. The **re0** group is a special group designator that is only used by **RE0** in a redundant routing platform.

```
[edit]
root# set groups re0
```

2. Navigate to the **groups re0** level of the configuration hierarchy.

```
[edit]
root# edit groups re0
```

3. Specify the router hostname.

```
[edit groups re0]
root# set system host-name host-name
```



NOTE: The hostname specified in the router configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, the hostname appears at the command-line prompt when the user is logged in to the CLI:

```
user-name@host-name>
```

4. Configure the IP address and prefix length for the router Ethernet interface.

- For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces em0 unit 0 family inet address address/prefix-length
```

To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

- For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

5. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

6. Create the configuration group **re1**.

```
[edit]
root# set groups re1
```

7. Navigate to the **groups re1** level of the configuration hierarchy.

```
[edit]
root# edit groups re1
```

8. Specify the router hostname.

```
[edit groups re1]
root# set system host-name host-name
```

9. Configure the IP address and prefix length for the router Ethernet interface.

- For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only:

```
[edit]
root@# set interfaces em0 unit 0 family inet address address/prefix-length
```

To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

- For a T1600 standalone router (not connected to a TX Matrix Plus router, and not in a routing matrix):

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

10. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

11. Specify the group application order.

```
[edit]
root# set apply-groups [ re0 re1 ]
```

Complete the Management Console Configuration

To configure the global management console parameters.

1. Configure the IP address of the DNS server.

```
[edit]
root# set system name-server address
```

2. Configure the router domain name.

```
[edit]
root# set system domain-name domain-name
```

3. Configure the IP address of a backup router. The backup router is used while the local router is booting and if the routing process fails to start. Once the routing process starts, the backup router address is removed from the local routing and forwarding tables. For more information about the backup router, see the *Getting Started Guide for Routing Devices*.

```
[edit]
root# set system backup-router address
```

4. (Optional) Configure the static routes to remote subnets with access to the management port. Access to the management port is limited to the local subnet. To access the management port from a remote subnet, you need to add a static route to that subnet within the routing table.

```
[edit]
root# set routing-options static route remote-subnet next-hop destination-IP retain
no-readvertise
```

5. Configure telnet service at the **[edit system services]** hierarchy level.

```
[edit]
root# set system services telnet
```

Commit and Synchronize Changes

Commit the configuration changes. When you issue the **synchronize** command, the configuration is shared between both Routing Engines and committed on both Routing Engines simultaneously.

1. Before committing the configuration, you can review the configuration entries using the **show** command.

```

root# show
## Last changed: 2008-10-17 18:32:25 UTC
version 9.1R1.8;
groups {
  re0 {
    system {
      host-name spice-re0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.69.155/21;
          }
        }
      }
    }
  }
  re1 {
    system {
      host-name spice-re1;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.70.72/21;
          }
        }
      }
    }
  }
}
global;
}
apply-groups [ re0 re1 ];
system {
  domain-name devicex.example.com;
  backup-router 192.168.71.254;
  root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
  }
  name-server {
    192.168.1.1;
  }
  login {
    user user1 {
      uid 2001;
      class super-user;
      authentication {
        encrypted-password "$ABC123"; ## SECRET-DATA
      }
    }
  }
}

```

```
    }  
  }  
  services {  
    telnet;  
  }  
  syslog {  
    user * {  
      any emergency;  
    }  
    file messages {  
      any notice;  
      authorization info;  
    }  
    file interactive-commands {  
      interactive-commands any;  
    }  
  }  
}  
routing-options {  
  static {  
    /* corporate office */  
    route 172.16.0.0/12 {  
      next-hop 192.168.71.254;  
      retain;  
      no-readvertise;  
    }  
  }  
}
```

2. Commit and synchronize the configuration. The **commit synchronize** command commits this new configuration on both Routing Engines simultaneously.

```
[edit]  
root# commit synchronize  
re0:  
configuration check succeeds  
re1:  
commit complete  
re0:  
commit complete
```

If you receive an error message after you issue the **commit** statement, you can review the configuration using the **show** command to find the errors in your configuration. You can delete incorrect entries using the **delete** command. For example, to delete a hostname from the configuration, issue the following command:

```
[edit]  
root# delete system host-name host-name
```

3. Exit configuration mode.

```
[edit]  
root# exit  
Exiting configuration mode  
  
root>
```

Saving a Rescue Configuration File

A rescue configuration file is helpful in the event that your device's configuration file has been misconfigured. You can restore the device to this rescue configuration to bring the device back online. If you save this file off the device, the rescue configuration can also be used to restore your device in the event of a software failure.

To save a current device configuration as a rescue configuration file:

1. Edit the configuration file on the device to reflect the base configuration you wish to use.

For more information about editing the configuration, see *Overview for Routing Devices*.

2. In the CLI operational mode, save this edited base configuration as the rescue configuration file:

```
user@host> request system configuration rescue save
```

The rescue configuration file is automatically saved under **/config** directory.

3. Copy the rescue configuration to a remote server:

```
user@host1> cd /config/
user@host1> ls -ltr rescue.conf.gz

user@host1 ftp host2
Name: username
Password: password
User user logged in.
ftp> cd /var/tmp
ftp> lcd /config
ftp> bi
ftp> put rescue.conf.gz
local: rescue.conf.gz remote: rescue.conf.gz

Transfer complete.
ftp> bye
Goodbye.
```

To roll back to the rescue configuration, use the **rollback rescue** command.

```
user@host# rollback rescue
```

```
load complete
```



NOTE: After rolling back to the rescue configuration, you must commit the configuration to activate it:

```
user@host#commit
```

Restoring a Saved Configuration

To restore a saved configuration, perform the following tasks:

1. [Copy Saved Files to the Router on page 184](#)
2. [Loading and Committing the Configuration File on page 184](#)

Copy Saved Files to the Router

To copy the saved configuration to the router:

1. Log in to the console as **root**. There is no password.

```
Escape character is '^['.  
[Enter]  
router (ttyd0)
```

```
login: root  
Password: [Enter]
```

Initially, access to the router is limited to the console port after a recovery installation. Access through the management ports and interfaces is set in the configuration. For information about accessing the router through the console port, see the administration guide for your particular router.

2. Start the CLI:

```
# cli
```

3. Copy the configuration file on the remote server to the router's **/var/tmp** directory:

```
root@host> ftp remote-server  
user: username  
password: password  
ftp> bin  
Type set to I.  
ftp> get /path/file  
ftp> bye  
Goodbye.
```

Loading and Committing the Configuration File

Once the saved configuration file is copied to the router, you load and commit the file:

1. Start the CLI configuration mode.

```
user@routername> configure  
Entering configuration mode
```

```
[edit]  
user@host#
```

2. Load the file into the current configuration. You should override the existing file.

```
user@host#  
load override /var/tmp/filename  
load complete
```

3. Commit the file.


```
user@host# commit
commit complete
```

4. Exit the CLI configuration mode.

```
user@host# exit
user@host>
```

5. Back up Junos OS.

After you have installed the software on the router, committed the configuration, and are satisfied that the new configuration is successfully running, issue the **request system snapshot** command to back up the new software to the **/altconfig** file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The **request system snapshot** command causes the root file system to be backed up to **/altroot**, and **/config** to be backed up to **/altconfig**. The root and **/config** file systems are on the router's CompactFlash card, and the **/altroot** and **/altconfig** file systems are on the router's hard disk or solid-state drive (SSD).

Reverting to the Default Factory Configuration by Using the **request system zeroize** Command

The **request system zeroize** command is a standard Junos OS operational mode command that removes all configuration information and resets all key values. The operation unlinks all user-created data files, including customized configuration and log files, from their directories. The switch then reboots and reverts to the factory-default configuration.

To completely erase user-created data so that it is unrecoverable, use the **request system zeroize media** command.



CAUTION: Before issuing **request system zeroize**, use the **request system snapshot** command to back up the files currently used to run the switch to a secondary device.

To revert to the factory-default configuration by using the **request system zeroize** command:

1. `user@switch> request system zeroize`
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (yes)
2. Type **yes** to remove configuration and log files and revert to the factory default configuration.
3. Complete the initial configuration of the switch.

Related Documentation • [request system zeroize on page 377](#)

Reverting to the Rescue Configuration

If someone inadvertently commits a configuration that denies management access to a device and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration. The rescue configuration is a previously committed, valid configuration.

To revert the switch to the rescue configuration:

1. Enter the **load override** command.

```
[edit]  
user@switch# load override filename
```

2. Commit your changes.

```
[edit]  
user@switch# commit filename
```

Related Documentation

- *Reverting to the Default Factory Configuration*

Reinstalling Software

- [Checklist for Reinstalling Junos OS on page 187](#)
- [Log the Software Version Information on page 189](#)
- [Log the Hardware Version Information on page 190](#)
- [Log the Chassis Environment Information on page 191](#)
- [Log the System Boot-Message Information on page 192](#)
- [Log the Active Configuration on page 194](#)
- [Log the Interfaces on the Router on page 194](#)
- [Log the BGP, IS-IS, and OSPF Adjacency Information on page 195](#)
- [Log the System Storage Information on page 196](#)
- [Back Up the Currently Running and Active File System on page 197](#)
- [Reinstall Junos OS on page 197](#)
- [Reconfigure Junos OS on page 198](#)
- [Configure Host Names, Domain Names, and IP Addresses on page 202](#)
- [Protecting Network Security by Configuring the Root Password on page 204](#)
- [Check Network Connectivity on page 206](#)
- [Copy Backup Configurations to the Router on page 206](#)
- [After You Reinstall Junos OS on page 206](#)
- [Compare Information Logged Before and After the Reinstall on page 207](#)
- [Back Up the New Software on page 207](#)

Checklist for Reinstalling Junos OS

Table 26 provides links and commands for reinstalling Junos OS.

Table 26: Checklist for Reinstalling Junos OS

Tasks	Command or Action
Before You Reinstall Junos OS	
1. Log the Software Version Information on page 189	<code>show version</code> <i>save filename</i>

Table 26: Checklist for Reinstalling Junos OS *(continued)*

Tasks	Command or Action
2. Log the Hardware Version Information on page 190	<code>show chassis hardware</code> <i>save filename</i>
3. Log the Chassis Environment Information on page 191	<code>show chassis environment</code> <i>save filename</i>
4. Log the System Boot-Message Information on page 192	<code>show system boot-messages</code> <i>save filename</i>
5. Log the Active Configuration on page 194	<code>show configuration</code> <i>save filename</i>
6. Log the Interfaces on the Router on page 194	<code>show interface terse</code> <i>save filename</i>
7. Log the BGP, IS-IS, and OSPF Adjacency Information on page 195	<code>show bgp summary</code> <i>save filename</i> <code>show isis adjacency brief</code> <i>save filename</i> <code>show ospf neighbor brief</code> <i>save filename</i>
8. Log the System Storage Information on page 196	<code>show system storage</code> <i>save filename</i>
9. Back Up the Currently Running and Active File System on page 197	<code>request system snapshot</code>
10.	http://www.juniper.net/support
“Reinstall Junos OS” on page 197	
Insert the floppy and reboot the system.	
“Reconfigure Junos OS” on page 198	
1. Configure Host Names, Domain Names, and IP Addresses on page 198	Log in as root. Start the CLI. Enter configuration mode: <code>configure</code> <code>set system host-name <i>host-name</i></code> <code>set system domain-name <i>domain-name</i></code> <code>set interfaces fxp0 unit 0 family inet address <i>address/prefix-length</i></code> <code>set system backup-router <i>address</i></code> <code>set system name-server <i>address</i></code>
2. Protecting Network Security by Configuring the Root Password on page 200	<code>set system root-authentication plain-text-password</code> <code>set system root-authentication encrypted-password <i>password</i></code> <code>set system root-authentication ssh-rsa <i>key</i></code> <code>commit</code> <code>exit</code>
3. Check Network Connectivity on page 201	<code>ping <i>address</i></code>
4. Copy Backup Configurations to the Router on page 202	<code>file copy var/tmp</code> <code>configure</code> [edit] <code>load merge /config/<i>filename</i></code> or <code>load replace /config/<i>filename</i></code> [edit] <code>commit</code>

Table 26: Checklist for Reinstalling Junos OS (*continued*)

Tasks	Command or Action
“After You Reinstall Junos OS” on page 206	
1. Compare Information Logged Before and After the Reinstall on page 206	show version save <i>filename</i> show chassis hardware save <i>filename</i> show chassis environment save <i>filename</i> show system boot-messages save <i>filename</i> show configuration save <i>filename</i> show interfaces terse save <i>filename</i> show bgp summary show isis adjacency brief show ospf neighbor brief save <i>filename</i> show system storage save <i>filename</i>
2. Back Up the New Software on page 207	request system snapshot

Log the Software Version Information

Action To log the Junos OS version information, use the following Junos OS CLI operational mode command:

```
user@host> show version | save filename
```

Sample Output `user@host> show version | save test`
Wrote 39 lines of output to 'test'

```
user@host> show version
Hostname:  my-router.net
Model:  m10
JUNOS Base OS boot [5.0R5]
JUNOS Base OS Software Suite [5.0R5]
JUNOS Kernel Software Suite [5.0R5]
JUNOS Routing Software Suite [5.0R5]
JUNOS Packet Forwarding Engine Support [5.0R5]
JUNOS Crypto Software Suite [5.0R5]
JUNOS Online Documentation [5.0R5]
KERNEL 5.0R5 #0 built by builder on 2002-03-02 05:10:28 UTC
MGD release 5.0R5 built by builder on 2002-03-02 04:45:32 UTC
CLI release 5.0R5 built by builder on 2002-03-02 04:44:22 UTC
CHASSISD release 5.0R5 built by builder on 2002-03-02 04:43:37 UTC
DCD release 5.0R5 built by builder on 2002-03-02 04:42:47 UTC
RPD release 5.0R5 built by builder on 2002-03-02 04:46:17 UTC
SNMPD release 5.0R5 built by builder on 2002-03-02 04:52:26 UTC
MIB2D release 5.0R5 built by builder on 2002-03-02 04:45:37 UTC
APSD release 5.0R5 built by builder on 2002-03-02 04:43:31 UTC
VRRPD release 5.0R5 built by builder on 2002-03-02 04:52:34 UTC
ALARMD release 5.0R5 built by builder on 2002-03-02 04:43:24 UTC
PFED release 5.0R5 built by builder on 2002-03-02 04:46:06 UTC
CRAFTD release 5.0R5 built by builder on 2002-03-02 04:44:30 UTC
SAMPLED release 5.0R5 built by builder on 2002-03-02 04:52:20 UTC
ILMID release 5.0R5 built by builder on 2002-03-02 04:45:21 UTC
BPRELAYD release 5.0R5 built by builder on 2002-03-02 04:42:41 UTC
RMOPD release 5.0R5 built by builder on 2002-03-02 04:46:11 UTC
jkernel-dd release 5.0R5 built by builder on 2002-03-02 04:41:07 UTC
jroute-dd release 5.0R5 built by builder on 2002-03-02 04:41:21 UTC
jdocs-dd release 5.0R5 built by builder on 2002-03-02 04:39:11 UTC
```

Meaning The sample output shows the hostname, router model, and the different Junos OS packages, processes, and documents.

Log the Hardware Version Information

Purpose You should log hardware version information in the rare event that a router cannot successfully reboot and you cannot obtain the Routing Engine serial number. The Routing Engine serial number is necessary for Juniper Networks Technical Assistance Center (JTAC) to issue a return to manufacturing authorization (RMA). Without the Routing Engine serial number, an onsite technician must be dispatched to issue the RMA.

Action To log the router chassis hardware version information, use the following Junos OS CLI operational mode command:

```
user@host> show chassis hardware | save filename
```

Sample Output The output for the M-series routers varies depending on the chassis components of each router. All routers have a chassis, midplanes or backplanes, power supplies, and Flexible

PIC Concentrators (FPCs). Refer to the hardware guides for information about the different chassis components.

```
user@host> show chassis hardware | save test
Wrote 43 lines of output to 'test'
```

```
user@host> show chassis hardware
Item          Version  Part number  Serial number  Description
Chassis                               101          M160
Midplane      REV 02   710-001245   S/N AB4107
FPM CMB       REV 01   710-001642   S/N AA2911
FPM Display   REV 01   710-001647   S/N AA2999
CIP           REV 02   710-001593   S/N AA9563
PEM 0         Rev 01   740-001243   S/N KJ35769    DC
PEM 1         Rev 01   740-001243   S/N KJ35765    DC
PCG 0         REV 01   710-001568   S/N AA9794
PCG 1         REV 01   710-001568   S/N AA9804
Host 1
MCS 1         REV 03   710-001226   S/N AA9777
SFM 0 SPP     REV 04   710-001228   S/N AA2975
SFM 0 SPR     REV 02   710-001224   S/N AA9838      Internet Processor I
SFM 1 SPP     REV 04   710-001228   S/N AA2860
SFM 1 SPR     REV 01   710-001224   S/N AB0139      Internet Processor I
FPC 0         REV 03   710-001255   S/N AA9806      FPC Type 1
CPU           REV 02   710-001217   S/N AA9590
PIC 1         REV 05   750-000616   S/N AA1527      1x OC-12 ATM, MM
PIC 2         REV 05   750-000616   S/N AA1535      1x OC-12 ATM, MM
PIC 3         REV 01   750-000616   S/N AA1519      1x OC-12 ATM, MM
FPC 1         REV 02   710-001611   S/N AA9523      FPC Type 2
CPU           REV 02   710-001217   S/N AA9571
PIC 0         REV 03   750-001900   S/N AA9626      1x STM-16 SDH, SMIR
PIC 1         REV 01   710-002381   S/N AD3633      2x G/E, 1000 BASE-SX
FPC 2
CPU           REV 03   710-001217   S/N AB3329
PIC 0         REV 01                                1x OC-192 SM SR-2
```

Meaning The sample output shows the hardware inventory for an M160 router with a chassis serial number of 101. For each component, the output shows the version number, part number, serial number, and description.

Log the Chassis Environment Information

Action To log the router chassis environment information, use the following Junos OS CLI operational mode command:

```
user@host> show chassis environment | save filename
```

Sample Output The following example shows output from the `show chassis environment` command for an M5 router:

```
user@m5-host> show chassis environment | save test
Wrote 14 lines of output to 'test'
```

```
user@m5-host> show chassis environment
Class Item          Status  Measurement
Power Power Supply A  OK
        Power Supply B  OK
Temp  FPC Slot 0      OK      32 degrees C / 89 degrees F
```

	FEB	OK	31 degrees C / 87 degrees F
	PS Intake	OK	26 degrees C / 78 degrees F
	PS Exhaust	OK	31 degrees C / 87 degrees F
Fans	Left Fan 1	OK	Spinning at normal speed
	Left Fan 2	OK	Spinning at normal speed
	Left Fan 3	OK	Spinning at normal speed
	Left Fan 4	OK	Spinning at normal speed

Meaning The sample output shows the environmental information about the router chassis, including the temperature and information about the fans, power supplies, and Routing Engine.

Log the System Boot-Message Information

Action To log the system boot-message information, use the following Junos OS CLI operational mode command:

```
user@host> show system boot-messages | save filename
```



```

Sample Output user@host> show system boot-messages | save test
Wrote 80 lines of output to 'test'

user@host> show system boot-messages
Copyright (c) 1992-1998 FreeBSD Inc.
Copyright (c) 1996-2000 Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California. All rights reserved.

JUNOS 4.1-20000216-Zf8469 #0: 2000-02-16 12:57:28 UTC

tlim@device1.example.com:/p/build/20000216-0905/4.1/release_kernel/sys/compile/GENERIC
CPU: Pentium Pro (332.55-MHz 686-class CPU)
    Origin = "GenuineIntel" Id = 0x66a Stepping=10

Features=0x183f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,<b16>,<b17>,MMX,<b24>>
Teknor CPU Card Recognized
real memory = 805306368 (786432K bytes)
avail memory = 786280448 (767852K bytes)
Probing for devices on PCI bus 0:
chip0 <generic PCI bridge (vendor=8086 device=7192 subclass=0)> rev 3 class 60000
    on pci0:0:0
chip1 <Intel 82371AB PCI-ISA bridge> rev 1 class 60100 on pci0:7:0
chip2 <Intel 82371AB IDE interface> rev 1 class 10180 on pci0:7:1
chip3 <Intel 82371AB USB interface> rev 1 class c0300 int d irq 11 on pci0:7:2
smb0 <Intel 82371AB SMB controller> rev 1 class 68000 on pci0:7:3
pcic0 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int a irq 15 on pci0:13:0
TI1131 PCI Config Reg: [pci only][FUNC0 pci int]
pcic1 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int b irq 12 on pci0:13:1
TI1131 PCI Config Reg: [pci only][FUNC1 pci int]
fxp0 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 12 on
    pci0:16:0
chip4 <generic PCI bridge (vendor=1011 device=0022 subclass=4)> rev 4 class 60400
    on pci0:17:0
fxp1 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
    pci0:19:0
Probing for devices on PCI bus 1:mcs0 <Miscellaneous Control Subsystem> rev 12
class ff0000 int a irq 12 on pci1:13:0
fxp2 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
    pci1:14:0
Probing for devices on the ISA bus:
sc0 at 0x60-0x6f irq 1 on motherboard
sc0: EGA color <16 virtual consoles, flags=0x0>
ed0 not found at 0x300
ed1 not found at 0x280
ed2 not found at 0x340
psm0 not found at 0x60
sio0 at 0x3f8-0x3ff irq 4 flags 0x20010 on isa
sio0: type 16550A, console
sio1 at 0x3e8-0x3ef irq 5 flags 0x20000 on isa
sio1: type 16550A
sio2 at 0x2f8-0x2ff irq 3 flags 0x20000 on isa
sio2: type 16550A
pcic0 at 0x3e0-0x3e1 on isa
PC-Card ctlr(0) TI PCI-1131 [CardBus bridge mode] (5 mem & 2 I/O windows)
pcic0: slot 0 controller I/O address 0x3e0
npx0 flags 0x1 on motherboard
npx0: INT 16 interface
fdc0: direction bit not set

```

```
fdc0: cmd 3 failed at out byte 1 of 3
fdc0 not found at 0x3f0
wdc0 at 0x1f0-0x1f7 irq 14 on isa
wdc0: unit 0 (wd0): <SunDisk SDCFB-80>, single-sector-i/o
wd0: 76MB (156672 sectors), 612 cyls, 8 heads, 32 S/T, 512 B/S
wdc0: unit 1 (wd1): <IBM-DCXA-210000>
wd1: 8063MB (16514064 sectors), 16383 cyls, 16 heads, 63 S/T, 512 B/S
wdc1 not found at 0x170
wdc2 not found at 0x180
ep0 not found at 0x300
fxp0: Ethernet address 00:a0:a5:12:05:5a
fxp1: Ethernet address 00:a0:a5:12:05:59
fxp2: Ethernet address 02:00:00:00:00:01
swapon: adding /dev/wd1s1b as swap device
Automatic reboot in progress...
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd0s1e: clean, 9233 free (9 frags, 1153 blocks, 0.1% fragmentation)
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd1s1f: clean, 4301055 free (335 frags, 537590 blocks, 0.0% fragmentation)
```

Meaning The sample output shows the initial messages generated by the system kernel upon boot. This is the content of the `/var/run/dmesg.boot` file.

Log the Active Configuration

Action To log the active configuration on the router, use the following Junos OS CLI operational mode command:

```
user@host> show configuration | save filename
```

Sample Output user@host> show configuration | save test
Wrote 4076 lines of output to 'test'

```
user@host> show configuration
system {
  host-name lab8;
  domain-name device1.example.com;
  backup-router 10.1.1.254;
    time-zone America/Los_Angeles;
  default-address-selection;
    dump-on-panic;
  name-server {
  [...Output truncated...]
```

Meaning The sample output shows the configuration currently running on the router, which is the last committed configuration.

Log the Interfaces on the Router

Action To log the interfaces on the router, use the following Junos OS CLI operational mode command:

```
user@host> show interface terse | save filename
```

Sample Output user@host> show interfaces terse | save test
Wrote 81 lines of output to 'test'

```

user@host> show interfaces terse
Interface      Admin Link Proto Local Remote
at-1/3/0       up    up
at-1/3/0.0     up    up    inet  1.0.0.1    --> 1.0.0.2
               iso
fxp0           up    up
fxp0.0         up    up    inet  10.168.5.59/24
gre            down  up
ipip           down  up
lo0            up    up
lo0.0          up    up    inet  127.0.0.1    --> 0/0
               iso 47.0005.80ff.f800.0000.0108.0001.1921.6800.5059.00
so-1/2/0       up    down
so-1/2/1       down  down
so-1/2/2       down  down
so-1/2/3       down  down
so-2/0/0       up    up
so-2/0/0.0     up    up    inet  1.2.3.4      --> 1.2.3.5
               iso
[...Output truncated...]

```

Meaning The sample output displays summary information about the physical and logical interfaces on the router.

Log the BGP, IS-IS, and OSPF Adjacency Information

Purpose The following commands log useful information about Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF) protocols. If you have other protocols installed, such as Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), or Protocol Independent Multicast (PIM), you also might log summary information for them.

Action To log the protocol peer information, use the following Junos OS CLI operational mode commands:

```

user@host> show bgp summary | save filename
user@host> show isis adjacency brief | save filename
user@host> show ospf neighbor brief | save filename

```

Sample Output 1 user@host> show bgp summary | save test
Wrote 45 lines of output to 'test'

```

user@host> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State   Pending
inet.0          4          4          0          0          0          0
Peer           AS      InPkt    OutPkt    OutQ    Flaps Last Up/Dwn
State|#Active/Received/Damped..
9.9.3.1         2      2627      2628        0        0    21:50:12 4/4/0
0/0/0

```

Sample Output 2 user@host> show isis adjacency brief | save test
Wrote 7 lines of output to 'test'

```

user@host> show isis adjacency brief
IS-IS adjacency database:
Interface System      L State      Hold (secs) SNPA
so-1/0/0.0 1921.6800.5067 2 Up          13
so-1/1/0.0 1921.6800.5067 2 Up          25
so-1/2/0.0 1921.6800.5067 2 Up          20
so-1/3/0.0 1921.6800.5067 2 Up          19
so-2/0/0.0 1921.6800.5066 2 Up          19
so-2/1/0.0 1921.6800.5066 2 Up          17
so-2/2/0.0 1921.6800.5066 2 Up          20
so-2/3/0.0 1921.6800.5066 2 Up          20
so-5/0/0.0 ranier      2 Up          17

```

Sample Output 3 user@host> show ospf neighbor brief | save test
Wrote 10 lines of output to 'test'

```

user@host> show ospf neighbor brief
Address      Intf      State      ID          Pri  Dead
10.168.254.225 fxp3.0    2Way       10.250.240.32 128  36
10.168.254.230 fxp3.0    Full       10.250.240.8  128  38
10.168.254.229 fxp3.0    Full       10.250.240.35 128  33
10.1.1.129      fxp2.0    Full       10.250.240.12 128  37
10.1.1.131      fxp2.0    Full       10.250.240.11 128  38
10.1.2.1        fxp1.0    Full       10.250.240.9  128  32
10.1.2.81       fxp0.0    Full       10.250.240.10 128  33

```

Meaning Sample output 1 displays summary information about BGP and its neighbors. Sample output 2 displays information about IS-IS neighbors. Sample output 3 displays information about all OSPF neighbors.

Log the System Storage Information

Action To log the system storage statistics for the amount of free disk space in the router's file system, use the following Junos OS CLI operational mode command:

```
user@host> show system storage | save filename
```

Sample Output user@host> show system storage | save test
Wrote 14 lines of output to 'test'

```
user@host> show system storage
Filesystem 1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a  65687    26700   33733    44%      /
devfs        16        16        0   100%    /dev/
/dev/vn1     9310     9310        0   100%    /packages/mnt/jbase
/dev/vn2     8442     8442        0   100%    /packages/mnt/jkernel-5.0R5.1
/dev/vn3    11486    11486        0   100%    /packages/mnt/jpfe-5.0R5.1
/dev/vn4     5742     5742        0   100%    /packages/mnt/jroute-5.0R5.1
/dev/vn5     1488     1488        0   100%    /packages/mnt/jcrypto-5.0R5.1
/dev/vn6       792      792        0   100%    /packages/mnt/jdocs-5.0R5.1
mfs:2373    1015815        3  934547     0%    /tmp
/dev/ad0s1e  25263        11  23231     0%    /config
procfs        4         4        0   100%    /proc
/dev/ad1s1f  9825963  1811085  7228801    20%    /var
```

Meaning The sample output displays statistics about the amount of free disk space in the router's file system. Values are displayed in 1024-byte (1-KB) blocks.

Back Up the Currently Running and Active File System

Action To back up the currently running and active file system so that you can recover to a known, stable environment in case there is a problem during the reinstall, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

Sample Output user@host> request system snapshot
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
umount: /altconfig: not currently mounted
Copying /config to /altconfig.. (this may take a few minutes)
The following filesystems were archived: / /config

Meaning The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Reinstall Junos OS

Action To reinstall Junos OS, follow these steps:

1. Insert the removable medium (boot floppy) into the router.
2. Reboot the router, either by power-cycling it or by issuing the **request system reboot** command from the CLI.
3. At the following prompt, type **y**:

`WARNING: The installation will erase the contents of your disk. Do you wish to continue (y/n)?`

The router copies the software from the removable medium onto your system, occasionally displaying status messages. This can take up to 10 minutes.
4. Remove the removable medium when prompted.

The router reboots from the primary boot device on which the software is installed. When the reboot is complete, the router displays the login prompt.

Reconfigure Junos OS

Purpose After you have reinstalled the software, you must copy the router's configuration files back to the router. (You also can configure the router from scratch, as described in *Junos System Basics Configuration Guide*) However, before you can copy the configuration files, you must establish network connectivity.

To reconfigure the software, follow these steps:

1. [Configure Host Names, Domain Names, and IP Addresses on page 198](#)
2. [Protecting Network Security by Configuring the Root Password on page 200](#)
3. [Check Network Connectivity on page 201](#)
4. [Copy Backup Configurations to the Router on page 202](#)

Configure Host Names, Domain Names, and IP Addresses

Action To configure the machine name, domain name, and various addresses, follow these steps:

1. Log in as **root**. There is no password.
2. Start the CLI:

`root# cli`
`root@>`
3. Enter configuration mode:

`cli> configure`
`[edit]`
`root@#`
4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" "):

`[edit]`
`root@# set system host-name host-name`
5. Configure the machine's domain name:

```
[edit]  
root@# set system domain-name domain-name
```

6. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]  
root@# set interfaces fxp0 unit 0 family inet address address / prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]  
root@# set system backup-router address
```

8. Configure the IP address of a Domain Name Server (DNS) server:

```
[edit]  
root@# set system name-server address
```

Protecting Network Security by Configuring the Root Password

Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router.

After a new router is initially powered on, you log in as the user **root** with no password. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

To set the root password, you have a few options as shown in Step 1 of the following procedure.

- Enter a plain-text password that Junos OS encrypts.
- Enter a password that is already encrypted.
- Enter a secure shell (ssh) public key string.

The most secure options of these three are using an already encrypted password or an ssh public key string. Pre-encrypting your password or using a ssh public key string means the plain-text version of your password will never be transferred over the internet, protecting it from being intercepted by a man-in-the-middle attack.



.....

BEST PRACTICE: Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group to strengthen security, as shown in Step 2 of this procedure. This step uses a group called **global** as an example.

.....

To set the root password:

1. Use one of these methods to configure the root password:

- To enter a plain-text password that the system encrypts for you:

```
[edit groups global system]
root@# set root-authentication plain-text-password
New Password: type password here
Retype new password: retry password here
```

If you use a plain-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as **## SECRET-DATA** in the configuration.

- To enter a password that is already encrypted:



CAUTION: Do not use the `encrypted-password` option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

If you accidentally configure the `encrypted-password` option with a plain-text password or with blank quotation marks (""), you will not be able to log in to the device as root, and you will need to complete the root password recovery process.

```
[edit groups global system]
root@# set root-authentication encrypted-password password
```

- To enter an ssh public key string:

```
[edit groups global system]
root@# set root-authentication (ssh-dsa | ssh-eccdsa | ssh-rsa key)
```

2. (Optional) Strengthen security by only allowing root access from the console port.

```
[edit groups global system]
root@# set services ssh root-login deny
```

3. If you used a configuration group in Step 2, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

4. Commit the changes.

```
root@# commit
```

Check Network Connectivity

Purpose Establish that the router has network connectivity.

Action To check that the router has network connectivity, issue a **ping** command to a system on the network:

```
root@> ping address
```

If there is no response, verify that there is a route to the ***address*** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route. Once the backup configuration is loaded and committed, the static route is no longer needed and should be deleted.

Copy Backup Configurations to the Router

Action To copy backup configurations to the router, follow these steps:

1. To copy the existing configuration and any backup configurations back onto the router, use the **file copy** command. Place the files in the **/var/tmp** directory.

```
user@host> file copy var/tmp/filename
```

2. Load and activate the desired configuration:

```
root@> configure
[edit]
root@# load merge/config/filename or load replace/config/filename
[edit]
root@# commit
```

Configure Host Names, Domain Names, and IP Addresses

Action To configure the machine name, domain name, and various addresses, follow these steps:

1. Log in as **root**. There is no password.
2. Start the CLI:

```
root# cli
root@>
```

3. Enter configuration mode:

```
cli> configure
[edit]
root@#
```

4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" "):

```
[edit]
root@# set system host-name host-name
```

5. Configure the machine's domain name:

```
[edit]
root@# set system domain-name domain-name
```

6. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address / prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

[edit]

root@# **set system backup-router *address***

8. Configure the IP address of a Domain Name Server (DNS) server:

[edit]

root@# **set system name-server *address***

Protecting Network Security by Configuring the Root Password

Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router.

After a new router is initially powered on, you log in as the user **root** with no password. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

To set the root password, you have a few options as shown in Step 1 of the following procedure.

- Enter a plain-text password that Junos OS encrypts.
- Enter a password that is already encrypted.
- Enter a secure shell (ssh) public key string.

The most secure options of these three are using an already encrypted password or an ssh public key string. Pre-encrypting your password or using a ssh public key string means the plain-text version of your password will never be transferred over the internet, protecting it from being intercepted by a man-in-the-middle attack.



BEST PRACTICE: Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group to strengthen security, as shown in Step 2 of this procedure. This step uses a group called **global** as an example.

To set the root password:

1. Use one of these methods to configure the root password:

- To enter a plain-text password that the system encrypts for you:

```
[edit groups global system]
root@# set root-authentication plain-text-password
New Password: type password here
Retype new password: retype password here
```

If you use a plain-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as **## SECRET-DATA** in the configuration.

- To enter a password that is already encrypted:



CAUTION: Do not use the `encrypted-password` option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

If you accidentally configure the `encrypted-password` option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to complete the root password recovery process.

```
[edit groups global system]
root@# set root-authentication encrypted-password password
```

- To enter an ssh public key string:

```
[edit groups global system]
root@# set root-authentication (ssh-dsa | ssh-eccdsa | ssh-rsa key)
```

2. (Optional) Strengthen security by only allowing root access from the console port.

```
[edit groups global system]
root@# set services ssh root-login deny
```

3. If you used a configuration group in Step 2, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

4. Commit the changes.

```
root@# commit
```

Related Documentation

- *Accessing a Junos OS Device the First Time*
- [Understanding User Accounts on page 798](#)
- *Recovering the Root Password*

Check Network Connectivity

Purpose Establish that the router has network connectivity.

Action To check that the router has network connectivity, issue a **ping** command to a system on the network:

```
root@> ping address
```

If there is no response, verify that there is a route to the **address** using the **show route** command. If the address is outside your **fxp0** subnet, add a static route. Once the backup configuration is loaded and committed, the static route is no longer needed and should be deleted.

Copy Backup Configurations to the Router

Action To copy backup configurations to the router, follow these steps:

1. To copy the existing configuration and any backup configurations back onto the router, use the **file copy** command. Place the files in the **/var/tmp** directory.

```
user@host> file copy var/tmp/filename
```

2. Load and activate the desired configuration:

```
root@> configure
[edit]
root@# load merge/config/filename or load replace/config/filename
[edit]
root@# commit
```

After You Reinstall Junos OS

To verify that the new version of the Junos OS is running as expected after the reinstall, follow these steps:

1. [Compare Information Logged Before and After the Reinstall on page 206](#)
2. [Back Up the New Software on page 207](#)

Compare Information Logged Before and After the Reinstall

Purpose Compare the operation of the system before and after the reinstall to ensure that everything is working as expected.

Action To obtain system information, use the following commands:

```
user@host> show version
user@host> show chassis hardware
user@host> show chassis environment
user@host> show system boot-messages
user@host> show configuration
user@host> show interface terse
user@host> show bgp summary
```

```
user@host> show isis adjacency brief
user@host> show ospf neighbor brief
user@host> show system storage
```

Compare the information from these commands with the information you obtained before the reinstall.

Back Up the New Software

Purpose After a week or so, when you are satisfied that the new software is running successfully, we recommend that you back up the reinstalled software.

Action To back up the reinstalled software, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Compare Information Logged Before and After the Reinstall

Purpose Compare the operation of the system before and after the reinstall to ensure that everything is working as expected.

Action To obtain system information, use the following commands:

```
user@host> show version
user@host> show chassis hardware
user@host> show chassis environment
user@host> show system boot-messages
user@host> show configuration
user@host> show interface terse
user@host> show bgp summary
user@host> show isis adjacency brief
user@host> show ospf neighbor brief
user@host> show system storage
```

Compare the information from these commands with the information you obtained before the reinstall.

Back Up the New Software

Purpose After a week or so, when you are satisfied that the new software is running successfully, we recommend that you back up the reinstalled software.

Action To back up the reinstalled software, use the following Junos OS CLI operational mode command:

```
user@host> request system snapshot
```

The root file system is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's internal flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Downgrading Software

- [Downgrading Junos OS from Upgraded FreeBSD on page 209](#)

Downgrading Junos OS from Upgraded FreeBSD

Starting with Junos OS Release 15.1, certain hardware platforms run a Junos OS based on an upgraded FreeBSD kernel instead of older versions of FreeBSD. If you have previously upgraded to Junos OS with upgraded FreeBSD, you can downgrade to earlier versions of Junos OS, as long as the downgrade conforms to the Junos OS policy of skipping at most two earlier releases.

Before you begin:

1. Verify that you have previously upgraded to Junos OS with the upgraded FreeBSD kernel, as described in [“Upgrading Junos OS with Upgraded FreeBSD” on page 139](#).
2. Download the Junos OS package.

Select and perform the procedure that matches your conditions:

- [Downgrading from Junos OS with Upgraded FreeBSD to Junos OS on page 209](#)
- [Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD on page 211](#)

Downgrading from Junos OS with Upgraded FreeBSD to Junos OS

This example uses the package `/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz` to install Junos OS with a pre-upgraded FreeBSD kernel on the master Routing Engine (re0).



NOTE: The following procedure refers to routers, but it also applies to switches.

To downgrade from Junos OS with upgraded FreeBSD to Junos OS:

1. Enter the **request system software add *package-name* no-validate reboot** command from the operational mode in the CLI.

Use the **no-validate** and **reboot** options with the **request system software add** command. If you leave out the **no-validate** option, the command uses the **validate** option by

default, and direct validation of running configuration does not work for downgrading to Junos OS from Junos OS with upgraded FreeBSD.



NOTE: To validate current configuration on an downgrade to Junos OS from Junos OS with upgraded FreeBSD, use the `request system software validate on (Junos OS with Upgraded FreeBSD)` command.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.

The following example uses the **re0** option:

```
user@host>request system software add
/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz re0 no-validate reboot
THIS IS A SIGNED PACKAGE Saving the config files ...
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install Rebooting. Please wait ...
shutdown: [pid 11001] Shutdown NOW! *** FINAL System shutdown message
from root@host *** System going down IMMEDIATELY Shutdown NOW! System
shutdown time has arrived\x07\x07 users@host> Connection to
device1.example.com closed by remote host. Connection to
device1.example.com closed. ... user@router> show version
Hostname: host
Model: mx240
Junos: 13.3R2.7
JUNOS Base OS boot [13.3R2.7]
JUNOS Base OS Software Suite [13.3R2.7]
JUNOS Kernel Software Suite [13.3R2.7]
JUNOS Crypto Software Suite [13.3R2.7]
JUNOS Packet Forwarding Engine Support (M/T/EX Common) [13.3R2.7]
JUNOS Packet Forwarding Engine Support (MX Common) [13.3R2.7]
JUNOS Online Documentation [13.3R2.7]
JUNOS Services AACL Container package [13.3R2.7]
...
```

2. Verify the downgrade of the software package.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Downgrading from Junos OS with Upgraded FreeBSD to an Earlier Release of Junos OS with Upgraded FreeBSD

This example uses the package `/var/tmp/jinstall-13.3R2.7-domestic-signed.tgz` to install Junos OS with a pre-upgraded FreeBSD kernel on the master Routing Engine (**re0**).



NOTE: The following procedure refers to routers, but it also applies to switches.

To downgrade from Junos OS with upgraded FreeBSD to an earlier release of Junos OS with upgraded FreeBSD:

1. Enter the **request system software add *package-name* validate reboot** command from the operational mode in the CLI:

Use the **validate** and **reboot** options with the **request system software add** command. The command uses the **validate** option by default.

If you leave out the **reboot** option, you can take care of that in a separate reboot step.
2. Verify the downgrade of the software package.

```
user@host> show version
```



NOTE: The output shows the OS kernel, OS runtime, and other packages installed on the router.

Related Documentation

- [Upgrading Junos OS with Upgraded FreeBSD on page 139](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)
- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [request system reboot \(Junos OS with Upgraded FreeBSD\) on page 316](#)

CHAPTER 13

Rebooting or Halting Software Processes on a Device

- [Restarting and Halting SRX Series Devices on page 213](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 218](#)
- [Restarting the Chassis on SRX Series Devices on page 218](#)
- [Rebooting or Halting the EX Series Switch \(J-Web Procedure\) on page 219](#)

Restarting and Halting SRX Series Devices

This topic includes the following sections:

- [Rebooting SRX Series Devices on page 213](#)
- [Halting SRX Series Devices on page 215](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 217](#)
- [Restarting the Chassis on SRX Series Devices on page 217](#)

Rebooting SRX Series Devices

This example shows how to reboot a SRX Series device.

- [Requirements on page 213](#)
- [Overview on page 213](#)
- [Configuration on page 214](#)
- [Verification on page 215](#)

Requirements

Before rebooting the device, save and commit any Junos OS updates.

Overview

This example shows how to reboot a device fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

Configuration

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host> request system reboot at 5 in 50 media internal message stop
```

GUI Step-by-Step Procedure To reboot a device:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Reboot in 50 minutes** to reboot the device fifty minutes from the current time.
3. Select the **internal** (for SRX Series devices) boot device from the Reboot From Media list.
4. In the Message box, type **stop** as the message to display to any user on the device before the reboot occurs.
5. Click **Schedule**. The J-Web user interface requests confirmation to perform the reboot.
6. Click **OK** to confirm the operation.
 - If the reboot is scheduled to occur immediately, the device reboots. You cannot access J-Web until the device has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web login page.
 - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web user interface Reboot page.
7. Click **OK** to check your configuration and save it as a candidate configuration.
8. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To reboot a device:

From operational mode, schedule a reboot of the device to occur fifty minutes from when you set the time from the internal media while sending a text message of 'stop' to all system users before the device reboots.

Enter:

```
user@host> request system reboot at 5 in 50 media internal message stop
```

Results From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Device Reboot on page 215](#)

Verifying the Device Reboot

Purpose Verify that the device rebooted.

Action From operational mode, enter the **show system** command.

Halting SRX Series Devices

This example shows how to halt a device.

- [Requirements on page 215](#)
- [Overview on page 215](#)
- [Configuration on page 215](#)
- [Verification on page 216](#)

Requirements

Before halting the device, save and commit any Junos OS updates.

Overview

When the device is halted, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.



NOTE: If you cannot connect to the device through the console port, shut down the device by pressing and holding the power button on the front panel until the **POWER LED** turns off. After the device has shut down, you can power on the device by pressing the power button again. The **POWER LED** turns on during startup and remains steadily green when the device is operating normally.

This example shows how to halt the system and stop software processes on the device immediately.

Configuration

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, enter:

```
user@host>request system halt at now
```



NOTE: The **request system halt** command used for halting the system and stopping software processes on the device is not supported on SRX1500 devices.

GUI Step-by-Step Procedure

To halt a device immediately:

1. In the J-Web user interface, select **Maintain>Reboot**.
2. Select **Halt Immediately**. After the software stops, you can access the device through the console port only.
3. Click **Schedule**. The J-Web user interface requests confirmation to halt.
4. Click **OK** to confirm the operation. If the device halts, all software processes stop and you can access the device through the console port only. Reboot the device by pressing any key on the keyboard.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To halt a device:

From operational mode, halt the SRX Series device immediately.

```
user@host> request system halt at now
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the Device Halt on page 217](#)

Verifying the Device Halt

Purpose Verify that the device halted.

Action From operational mode, enter the **show system** command.

Bringing Chassis Components Online and Offline on SRX Series Devices

You can use the **request** commands to bring chassis components online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
```

Where **<fru>** in the request chassis command can be any of the following (for Branch SRX Series devices):

- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Where **<fru>** in the request chassis command can be any of the following (for High-End SRX Series devices):

- **cb**—Changes the control board status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine**—Changes the routing engine status.



NOTE: The **request chassis** command is not supported for bringing SPCs online and offline.

Example:

To bring specific pic and the corresponding fpc slot online, from operational mode enter the following **request chassis** command:

```
user@host> request chassis pic pic-slot 1 fpc-slot 1 online
```

Restarting the Chassis on SRX Series Devices

You can restart the chassis using the **restart chassis-control** command with the following options:

- To restart the process gracefully:

```
user@host> restart chassis-control gracefully
```

- To restart the process immediately:
`user@host> restart chassis-control immediately`
- To restart the process softly:
`user@host> restart chassis-control soft`

Bringing Chassis Components Online and Offline on SRX Series Devices

You can use the **request** commands to bring all chassis components (except Power Entry Modules and fans) online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

Where **<fru>** in the request chassis command can be any of the following:

- **cluster**—Changes the chassis cluster status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Related Documentation

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Junos OS Upgrade Methods on the SRX Series Devices](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Restarting the Chassis on SRX Series Devices on page 218](#)

Restarting the Chassis on SRX Series Devices

You can use the **request** commands to bring all chassis components (except Power Entry Modules and fans) online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

Where **<fru>** in the request chassis command can be any of the following:

- **cluster**—Changes the chassis cluster status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

Related Documentation

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 150](#)
- [Restarting the Chassis on SRX Series Devices on page 218](#)

Rebooting or Halting the EX Series Switch (J-Web Procedure)

You can use the J-Web interface to schedule a reboot or to halt the switching platform.

To reboot or halt the switching platform by using the J-Web interface:

1. In the J-Web interface, select **Maintain > Reboot**.
2. Select one:
 - **Reboot Immediately**—Reboots the switching platform immediately.
 - **Reboot in *number of minutes***—Reboots the switch in the number of minutes from now that you specify.
 - **Reboot when the system time is *hour:minute***—Reboots the switch at the absolute time that you specify, on the current day. You must select a 2-digit hour in 24-hour format and a 2-digit minute.
 - **Halt Immediately**—Stops the switching platform software immediately. After the switching platform software has stopped, you can access the switching platform through the console port only.
3. (Optional) In the Message box, type a message to be displayed to any users on the switching platform before the reboot occurs.
4. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
5. Click **OK** to confirm the operation.
 - If the reboot is scheduled to occur immediately, the switch reboots. You cannot access the J-Web interface until the switch has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
 - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
 - If the switch is halted, all software processes stop and you can access the switching platform through the console port only. Reboot the switch by pressing any key on the keyboard.

Related Documentation

- *Starting the J-Web Interface*

PART 3

Installing and Managing Software Licenses

- [Software License Overview on page 223](#)
- [Installing and Managing Licenses on page 257](#)

Software License Overview

- [Junos OS Feature Licenses on page 223](#)
- [License Enforcement on page 224](#)
- [Junos OS Feature License Keys on page 225](#)
- [Software Feature Licenses on page 228](#)
- [Understanding Software Licenses for EX Series Switches on page 246](#)

Junos OS Feature Licenses

Some Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to Junos OS feature licensing requirements, you must purchase one license per feature per device. The presence of the appropriate software license key on your device determines whether you are eligible to configure and use the licensed feature.

To speed deployment of licensed features, Junos OS software implements an honor-based licensing structure and provides you with a 30-day grace period to use a licensed feature without a license key installed. The grace period begins when you configure the feature and your device uses the licensed feature for the first time, but not necessarily when you install the license. After the grace period expires, the system generates system log messages saying that the feature requires a license. To clear the error message and use the licensed feature properly, you must install and verify the required license.

For information about how to purchase software licenses, contact your Juniper Networks sales representative.

Related Documentation

- [License Enforcement on page 224](#)
- [Junos OS Feature License Model Number for SRX Series Services Gateways on page 236](#)
- [Adding New Licenses \(CLI Procedure\) on page 257](#)
- [Deleting a License \(CLI Procedure\) on page 258](#)
- [Saving License Keys on page 259](#)
- [Verifying Junos OS License Installation on page 260](#)

License Enforcement

For features or scaling levels that require a license, you must install and properly configure the license to meet the requirements for using the licensable feature or scale level. The device enables you to commit a configuration that specifies a licensable feature or scale without a license for a 30-day grace period. The grace period is a short-term grant that enables you to start using features in the pack or scale up to the system limits (regardless of the license key limit) without a license key installed. The grace period begins when the licensable feature or scaling level is actually used by the device (not when it is first committed). In other words, you can commit licensable features or scaling limits to the device configuration, but the grace period does not begin until the device uses the licensable feature or exceeds a licensable scaling level.



NOTE: Configurations might include both licensed and nonlicensed features. For these situations, the license is enforced up to the point where the license can be clearly distinguished. For example, an authentication-order configuration is shared by both Authentication, Authorization, and Accounting (AAA), which is licensed, and by Layer 2 Tunneling Protocol (L2TP), which is not licensed. When the configuration is committed, the device does not issue any license warnings, because it is not yet known whether AAA or L2TP is using the configuration. However, at runtime, the device checks for a license when AAA authenticates clients, but does not check when L2TP authenticates clients.

The device reports any license breach as a warning log message whenever a configuration is committed that contains a feature or scale limit usage that requires a license. Following the 30-day grace period, the device periodically reports the breach to syslog messages until a license is installed and properly configured on the device to resolve the breach.



NOTE: Successful commitment of a licensable feature or scaling configuration does not imply that the required licenses are installed or not required. If a required license is not present, the system issues a warning message after it commits the configuration.

Related Documentation

- [Junos OS Feature Licenses on page 223](#)
- [Software Feature Licenses on page 228](#)
- [Adding New Licenses \(CLI Procedure\) on page 257](#)
- [Deleting a License \(CLI Procedure\) on page 258](#)
- [Saving License Keys on page 259](#)
- [Verifying Junos OS License Installation on page 260](#)

Junos OS Feature License Keys

Some Junos OS software features require a license to be activated. To enable each licensed feature, you must purchase, install, manage, and verify a license key that corresponds to the licensed feature.

Release-Tied License Keys and Upgrade Licenses on MX Series Routers

The Junos OS licensing infrastructure currently associates a license feature with attributes such as date, platform, and validity. In addition to these attributes, for MX Series routers running Junos OS Release 12.2 and later, a licensed feature can be associated with a release number at the time of generating the license key. This type of release-tied license key is used to validate a particular licensed feature while attempting a software upgrade. The upgrade process aborts if the release number in the license key is earlier than the Junos OS release number to which the system is being upgraded.

Additionally, an upgrade license key can be generated for a release-tied licensed feature. An upgrade license key is used for carrying forward a capacity license to the upgrade release. Although an upgrade license might be an acceptable license on the current release, it does not add to the existing capacity limit. The capacity added in the upgrade license key is valid for the upgrade software release only.

The release number embedded in the license key indicates the maximum release number up to which Junos OS can be upgraded.

As an example, assume that your system is running Junos OS Release 12.2 and is using the **scale-subscriber** licensed feature with a later release-tied upgrade license key installed. If you request a software upgrade to the later release of Junos OS, the software upgrade operation fails and the following error message is displayed:

```
mgd: error: No valid upgrade license found for feature 'scale-subscriber'.  
Aborting Software upgrade.  
Validation failed
```

In this example, to successfully upgrade to the later release of Junos OS, the release number included in the upgrade license key should be greater than or equal to the later release number. Also, you can perform software upgrades up to the previous release without any additional license keys to retain the existing scale limit.

**NOTE:**

When you install a release-tied license, the following apply:

- You can purchase an upgrade capacity license only if a base capacity license for the same scale-tier has already been generated or purchased.
- You cannot install an upgrade license if the capacity does not match any of the existing base capacity licenses on the system.
- The license installation fails when you install a lower release number license key on a higher software release number.
- A release-tied license can be installed on a Junos OS release number that is lower than or equal to the release number included in the license key. For example, a 12.2 license key is valid on Junos OS Release 12.1.
- An upgrade license is valid only on the target release number specified in the license key, but can be installed on an earlier Junos OS release. For example, a 4 K scale-tier upgrade license for Junos OS Release 12.2 can be installed on an earlier release, and the installed count of licenses remains unaltered.
- Release-tied licenses of the previous release are not deleted on upgrading Junos OS to a newer release version.

Licensable Ports on MX5, MX10, and MX40 Routers

Starting with Junos OS Release 12.2, license keys are available to enhance the port capacity on MX5, MX10, and MX40 routers up to the port capacity of an MX80 router. The MX5, MX10, and MX40 routers are derived from the modular MX80 chassis with similar slot and port assignments, and provide all functionality available on an MX80 router, but at a lower capacity. Restricting port capacity is achieved by making a set of MIC slots and ports licensable. MICs without a license are locked, and are unlocked or made usable by installing appropriate upgrade licenses.

The base capacity of a router is identified by the Ideeprom assembly ID (I2C ID), which defines the board type. However, the Junos OS licensing infrastructure allows the use of restricted ports without a license for a grace period of 30 days. After the grace period expires, the router reverts back to the base capacity if no upgrade license is purchased and installed for the locked ports. The I2C ID along with an upgrade license determine the final capacity of an MX5, MX10, or MX40 router.

The MX5, MX10, MX40, and MX80 routers support the following types of MICs:

- A built-in 10-Gigabit Ethernet MIC with four 10-Gigabit Ethernet ports
- Two front-pluggable MICs

A feature ID is assigned to every license upgrade for enhancing port capacity. [Table 27](#) displays the chassis types and their associated port capacity, I2C ID, base capacity, feature ID, feature name, and the final capacity after a license upgrade.

Table 27: Upgrade Licenses for Enhancing Port Capacity

Chassis Type	Port Capacity	I2C ID	Base Capacity	Feature ID and Feature Name	Upgrade Capacity
MX5	20G	0x556	Slot 1 • 1/MIC0	f1—MX5 to MX10 upgrade	Slot 1 and 2 • 1/MIC0 • 1/MIC1
MX10	40G	0x555	Slot 1 and 2 • 1/MIC0 • 1/MIC1	f2—MX10 to MX40 upgrade	Slot 2 and first 2 ports on Slot 0 • 1/MIC1 • First 2 ports on 0/MIC0
MX40	60G	0x554	Slot 1, Slot 2 and first 2 ports on Slot 0 • 1/MIC0 • 1/MIC1 • First 2 ports on 0/MIC0	f3—MX40 to MX80 upgrade	Slot 2 and all ports on Slot 0 • 1/MIC1 • All 4 ports on 0/MIC0

When installing an upgrade license for enhancing port capacity on MX5, MX10 and MX40 routers, consider the following:

- To upgrade an MX5 router to MX80 router capacity, licenses for all three features (f1, f2, f3) must be installed. All three features can be provided in a single license key.
- To upgrade an MX10 router to MX40 router capacity, installing a license key with f2 feature is sufficient.
- Non-applicable feature IDs in a license key reject the upgrade license. For example:
 - An f1 feature ID on an MX10 upgrade license key rejects the license.
 - Feature IDs f1 and f2 on an MX40 upgrade license key reject the entire license.

Port Activation on MX104 Routers

Starting with Junos OS Release 13.3, license keys are available to activate the ports on the MX104 router. MX104 routers have four built-in ports. By default, in the absence of valid licenses, all four built-in ports are deactivated. By installing licenses, you can activate any two of the four or all of the four built-in ports. For instance, you can install a license to activate the first two built-in ports (xe-2/0/0 and xe-2/0/1) or you can install a license to activate the next two built-in ports (xe-2/0/2 and xe-2/0/3). You can also install a license to activate all four built-in ports (xe-2/0/0, xe-2/0/1, xe-2/0/2, and xe-2/0/3). If you have already activated two of the built-in ports, you can install an additional license to activate the other two built-in ports on the MX104 router.

A feature ID is assigned to every license for activating the built-in ports on the MX104 router. The port license model with the feature ID is described in [Table 28](#).

Table 28: Port Activation License Model for MX104 Routers

Feature ID	Feature Name	Functionality
F1	MX104 2X10G Port Activate (0 and 1)	Ability to activate first two built-in ports (xe-2/0/0 and xe-2/0/1)
F2	MX104 2X10G Port Activate (2 and 3)	Ability to activate next two built-in ports (xe-2/0/2 and xe-2/0/3)

Both the features are also provided in a single license key for ease of use. To activate all four ports, you must either install the licenses for both the features listed in [Table 28](#) or the single license key for both features. If you install the single license key when feature IDs F1 and F2 are already installed, the license does not get rejected. Also, MX104 routers do not support the graceful license expiry policy. A graceful license expiry policy allows the use of a feature for a certain period of time (usually a grace period of 30 days), and reverts if the license for that feature is not installed after the grace period.

Related Documentation

- [Junos OS Feature Licenses on page 223](#)
- [License Enforcement on page 224](#)
- [Software Feature Licenses on page 228](#)
- [Verifying Junos OS License Installation on page 260](#)
- [show system license on page 398](#)

Software Feature Licenses

Each license is tied to one software feature pack, and that license is valid for only one device.

For information about how to purchase software licenses, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

- [Software Features That Require Licenses on M Series, MX Series, and T Series Routers on page 228](#)
- [Software Features That Require Licenses on M Series Routers Only on page 231](#)
- [Software Features That Require Licenses on MX Series Routers Only on page 232](#)
- [Software Feature Licenses for SRX Series Devices on page 236](#)
- [Software Features That Require Licenses on EX Series Switches on page 241](#)
- [Software Features That Require Licenses on the QFX Series on page 243](#)

Software Features That Require Licenses on M Series, MX Series, and T Series Routers

[Table 29](#) lists the licenses you can purchase for each M Series, MX Series, and T Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 29: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers

Licensed Software Feature	Supported Devices	Model Number
Generalized Multi-Protocol Label Switching (GMPLS) Support on Junos OS	M10i, M7i, M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-GMPLS
IPv6 Support on Junos OS	M120, M160, M20, M320, M40e, T320, T640, and MX Series Routers	JS-IPv6
Logical Router Support for Junos OS	M10i, M120, M160, M20, M320, M40e, M7i, T320, T640, and MX Series Routers	JS-LR
J- Flow accounting license for Adaptive Services (AS) PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-ACCT
Chassis license for Application Traffic Optimization service, policy enforcement and application statistics. This license includes S-AI and S-LDPF functionality, and 1 Year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-ATO
Software License for Passive Monitoring Flow Collector Application, supporting 100Kpps throughput; Chassis based license for Multiservices PIC.	M320, T640, T320, T1600	S-COLLECTOR-100K
License to use Compressed Real-Time Transport Protocol (CRTP) feature in AS PIC and Multiservices PIC	M10i, M120, M160, M20, M320, M40e, M7i, T320, M10, M5, T640, and T1600	S-CRTP
Software License for Passive Monitoring DFC Application, supporting 100Kpps throughput; Chassis based license for Multiservices PIC	M320, T640, T320, T1600	S-DFC-100K
Security Services license for AS PIC and Multiservices PIC	M10i, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10, T1600	S-ES
Chassis license for IDP service, policy enforcement. This license includes S-AI and S-LDPF functionality, and 1 Year Signature Subscription License	MX104, MX240, MX480, MX960, M Series, and T Series Routers	S-IDP
Junos-FIPS Software License	M10i, M7i, M320, M40e, T320, T640	S-JUNOS-FIPS
Link Services Software License—up to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices Dense Port Concentrator (DPC)	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-1023

Table 29: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Link Services Software Upgrade License—from 255 to 1023 ML bundles per Chassis for Multiservices PIC and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-1023-UPG
Link Services Software Upgrade License—from 64 to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-255-UPG
Link Services Software License—up to 255 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, MX960	S-LSSL-256
Link Services Software License—up to 4 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M10i, M120, M20, M320, M40e, M7i, T320, M10, M5, T640, T1600, MX240, MX480, MX960	S-LSSL-4
Link Services Software License—up to 64 ML bundles per Chassis for AS PIC, MS PIC and MS DPC	M10, M7i, M5, M120, M20, M320, M40e, T320, T640, M10i, T1600, MX240, MX480, MX960	S-LSSL-64
Link Services Software Upgrade License—from 4 to 64 ML bundles per Chassis for AS PIC, Multiservices PIC, and Multiservices DPC	M5, M7i, M10, M10i, M20, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960	S-LSSL-64-UPG
Software License for Passive Monitoring Flow Monitor Application, supporting 1M flows. Chassis based license for Multiservices PIC	M320, T640, T320, T1600	S-MONITOR-1M
Network Address Translation (NAT), FW license on AS PIC and Multiservices PIC: Multi-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-NAT-FW-MULTI
NAT, FW license on AS PIC and Multiservices PIC: Single-instance	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-NAT-FW-SINGLE
Software license for Packet trigger subscriber policy	MX240, MX480, MX960, M120, M320	S-PTSP
Subscriber Access Feature Pack License Scaling (128000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (32000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (4000)	MX104, MX240, MX480, MX960, M120, M320, MX80	S-SA-4K
Subscriber Access Feature Pack License Scaling (64000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-64K

Table 29: Junos OS Feature License Model Number for M Series, MX Series, and T Series Routers (continued)

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License Scaling (8000)	MX104, MX240, MX480, MX960, M120, M320, MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (96000)	MX104, MX240, MX480, MX960, M120, M320	S-SA-96K
Subscriber Access Feature Pack license	MX104, MX240, MX480, MX960, M120, M320	S-SA-FP
Stateful Failover for Services on AS PIC and Multiservices PIC: Multilink PPP (MLPPP) only	M10, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, M10i, T1600	S-SERVICES-SFO
Subscriber Service Management Feature Packet License (RADIUS/SRC based Service Activation and Deactivation) Per-Service Accounting Features for Subscribers	MX104, MX240, MX480, MX960, M120, M320	S-SSM-FP
Subscriber Traffic Lawful Intercept Feature Pack License	MX240, MX480, MX960, M120, M320, MX80	S-SSP-FP
Software license for application aware traffic direct feature	MX240, MX480, MX960, M120, M320	S-TFDIRECT-APP
Software license for subscriber aware traffic direct feature	MX240, MX480, MX960, M120, M320	S-TFDIRECT-SUB
Video Services Feature Pack license	M120, M320, MX80, MX104, MX240, MX480, MX960	S-VIDEO-FP
Port capacity enhancement Feature Pack License for MX5 routers	MX5	mx5-to-mx10-upgrade
Port capacity enhancement Feature Pack License for MX10 routers	MX10	mx10-to-mx40-upgrade
Port capacity enhancement Feature Pack License for MX40 routers	MX40	mx40-to-mx80-upgrade

Software Features That Require Licenses on M Series Routers Only

Table 30 lists the licenses you can purchase for each M Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 30: Junos OS Feature License Model Number for M Series Routers

Licensed Software Feature	Supported Devices	Model Number
J-Flow accounting license on Integrated Adaptive Services Module (ASM) and Integrated Multi-Services Module	M7i	S-ACCT-BB
Security Services license on ASM and Integrated Multi-Services Module	M7i	S-ES-BB
Layer 2 Tunneling Protocol (L2TP) L2TP Network Server (LNS) license for 16000 sessions on Multiservices PIC	M120	S-LNS-16K
L2TP LNS license Upgrade—from 8000 to 16000 sessions on Multiservices PIC	M120	S-LNS-16K-UPG
L2TP LNS license for 2000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-2K
L2TP LNS license for 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-4K
L2TP LNS license Upgrade—from 2000 to 4000 sessions on AS PIC or Integrated Adaptive Services Module and Multiservices PIC	M7i, M10i, M120	S-LNS-4K-UPG
L2TP LNS license for 8000 sessions on Multiservices PIC	M7i, M10i, M120	S-LNS-8K
L2TP LNS license Upgrade—from 4000 to 8000 sessions on AS PIC and Multiservices PIC	M7i, M10i, M120	S-LNS-8K-UPG
Link services software license on integrated ASM and Integrated Multi Services Module—up to 4 ML bundles	M7i	S-LSSL-BB
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Multi instance	M7i	S-NAT-FW-MULTI-BB
NAT, FW license on Integrated ASM and Integrated Multi Services Module: Single instance	M7i	S-NAT-FW-SINGLE-BB
Tunnel services software license for AS PIC and Multiservices PIC (chassis license)	M7i, M10i	S-TUNNEL

Software Features That Require Licenses on MX Series Routers Only

Table 31 lists the licenses you can purchase for each MX Series software feature. Each license allows you to run the specified software feature on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 31: Junos OS Feature License Model Number for MX Series Routers

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX80-10G-ADV to MX80-40G-ADV	MX80	MX80-10G40G-UPG-ADV-B
Upgrade license—from MX80-10G to MX80-40G	MX80	MX80-10G40G-UPG-B
Upgrade license—from MX80-40G-ADV to full MX80	MX80	MX80-40G-UPG-ADV-B
Upgrade license—from MX80-40G to full MX80	MX80	MX80-40G-UPG-B
Upgrade license—from MX80-5G-ADV to MX80-10G-ADV	MX80	MX80-5G10G-UPG-ADV-B
Upgrade license—from MX80-5G to MX80-10G	MX80	MX80-5G10G-UPG-B
Upgrade license to activate 2x10GE P2&3	MX104	S-MX104-ADD-2X10GE
Upgrade license to activate 2X10GE P0&1	MX104	S-MX104-UPG-2X10GE
Upgrade license to activate 4X10GE fixed ports on MX104	MX104	S-MX104-UPG-4X10GE
License to support per VLAN queuing on MX104	MX104	S-MX104-Q
Chassis-based software license for inline J-Flow monitoring on MX5, MX10, M40, MX80, and MX104 Series routers	MX5, MX10, M40, MX80, and MX104	S-JFLOW-CH-MX5-104
Flow monitoring and accounting features using J-Flow service on any Modular Port Concentrator (MPC) or MS-DPC	MX240, MX480, MX960	S-ACCT-JFLOW-CHASSIS
Software License for in-line J-Flow service on Trio MPCs	MX240, MX480, MX960	S-ACCT-JFLOW-IN
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G
Flow monitoring and accounting features using J-Flow service on any MPC limited to 10G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-10G-UPG
Flow monitoring and accounting features using J-Flow service on any MPC limited to 5G of total JFLOW traffic	MX80	S-ACCT-JFLOW-IN-5G
2000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-2K
4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-4K
Upgrade from 2000 IKE sessions to 4000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-4K-UPG
6000 IKE sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-6K

Table 31: Junos OS Feature License Model Number for MX Series Routers (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Upgrade from 4000 IKE sessions to 6000 IKE Sessions on MS-DPC; Chassis based, limited to 6000 per Chassis	MX240, MX480, MX960	S-ES-6K-UPG
License to support DS3 Channelization (down to DS0) on each Modular Interface Card (MIC) for MIC-3D-8DS3-E3; also requires license S-MX80-Q when used on the MX80 platform	MX80, MX104, MX240, MX480, MX960	S-MIC-3D-8CHDS3
License to support full-scale L3 routes and L3 VPN	MX80	S-MX80-ADV-R
License to support 256K routes	MX104	S-MX104-ADV-R1
License to support scaling L3 and VPN routes to 1 million or more entries on MX104 platforms	MX104	S-MX104-ADV-R2
License to support full-scale L3 routes and L3 VPN on each slot for MPC-3D-16XGE-SFPP	MX240, MX480, MX960	S-MPC-3D-16XGE-ADV-R
License to support full-scale L3 routes and L3 VPN on each slot for port queuing MPCs	MX240, MX480, MX960	S-MPC-3D-PQ-ADV-R
License to support full-scale L3 routes and L3 VPN on each slot for hierarchical quality of service (HQoS) MPCs	MX240, MX480, MX960	S-MPC-3D-VQ-ADV-R
Subscriber Management Feature Pack License for MX80	MX80	S-MX80-SA-FP
Subscriber Management Feature Pack for MX104 series	MX104	S-MX104-SA-FP
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX80	S-MX80-SSM-FP
Subscriber Service Management Feature Packet License	MX104	S-MX104-SSM-FP
Upgrade to Traffic Direct Advanced (per MS-DPC)	MX960	S-MX-TD-UPG
License to run one instance of the NAT software on one NPU per MS-DPC	MX240, MX480, MX960	S-NAT
License to support inline NAT software on MX5, MX10, MX40, MX80, MX104	MX5, MX10, MX40, MX80, MX104	S-NAT-IN-MX5-104 (Replaces S-NAT-IN-MX40-MX80 and S-NAT-IN-MX5-MX10)
License to run one instance of the NAT software on one NPU per MS-MIC, MS-DPC, or MS-MPC	MX80, MX104, MX240, MA480, MX960, MX2010, MX2020	S-NAT-NPU (Replaces S-NAT-IN-MX40-MX80-UPG)
License to run NAT using any MPC in an MX Chassis	MX240, MX480, MX960	S-NAT-IN-MX-CHASSIS
Subscriber Access Feature Pack License Scaling (4000)	MX240, MX480, MX960, M120, M320, MX80	S-SA-4K

Table 31: Junos OS Feature License Model Number for MX Series Routers (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Subscriber Access Feature Pack License Scaling (8000)	MX240, MX480, MX960, M120, M320, MX80	S-SA-8K
Subscriber Access Feature Pack License Scaling (16,000)	MX240, MX480, MX960, MX80	S-SA-16K
Subscriber Access Feature Pack License Scaling (32,000)	MX240, MX480, MX960, M120, M320	S-SA-32K
Subscriber Access Feature Pack License Scaling (64,000)	MX240, MX480, MX960, M120, M320	S-SA-64K
Subscriber Access Feature Pack License Scaling (96,000)	MX240, MX480, MX960, M120, M320	S-SA-96K
Subscriber Access Feature Pack License Scaling (128,000)	MX240, MX480, MX960, M120, M320	S-SA-128K
Subscriber Access Feature Pack License Scaling (256,000)	MX240, MX480, MX960	S-SA-256K
Subscriber Access Feature Pack License	MX240, MX480, MX960, M120, M320	S-SA-FP
Software License for Secure Flow Mirroring Service (FlowTap) (does not require MS-DPC)	MX80, MX104, MX240, MX480, MX960	S-SFM-FLOWTAP-IN
License to run one instance of the SFW and software on a MS-DPC	MX960, MX480, MX240	S-SFW
Subscriber Service Management Feature Packet License—RADIUS and SRC-based service activation and deactivation per-service accounting features	MX240, MX480, MX960, M120, M320	S-SSM-FP
Software license for one member of an MX Virtual Chassis	MX960, MX480, MX240	S-VCR
Upgrade license—from MX10 to equivalent of MX40; allows additional 2x10G fixed ports to be used on the MX10 router	MX10-T	MX10-40-UPG
Upgrade license—from MX10 to equivalent of MX80; allows additional 4x10G fixed ports to be used on the MX10 router	MX10-T	MX10-80-UPG
Upgrade license—from MX40 to equivalent of MX80; allows additional 2x10G fixed ports to be used on the MX40 router	MX40-T	MX40-80-UPG
Upgrade license—from MX5 to equivalent of MX10; allows second MIC slot to be used on the MX5 router	MX5-T	MX5-10-UPG
Upgrade license—from MX5 to equivalent of MX40; allows second MIC slot and 2x10G fixed ports to be used on the MX5 router	MX5-T	MX5-40-UPG

Table 31: Junos OS Feature License Model Number for MX Series Routers (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Upgrade license—from MX5 to equivalent of MX80. Allows second MIC slot and 4x10G fixed ports to be used on the MX5 router	MX5-T	MX5-80-UPG
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 4000 through 8000 subscribers	MX80, MX960, MX480, MX240	S-SA-UP-8K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 8000 through 16,000 subscribers	MX80, MX960, MX480, MX240	S-SA-UP-16K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 16,000 through 32,000 subscribers	MX240, MX480, MX960	S-SA-UP-32K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 32,000 through 64,000 subscribers	MX240, MX480, MX960	S-SA-UP-64K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 64,000 through 96,000 subscribers	MX240, MX480, MX960	S-SA-UP-96K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 96,000 through 128,000 subscribers	MX240, MX480, MX960	S-SA-UP-128K
Upgrade license—Subscriber Access Feature Pack scaling license upgrade from 128,000 through 256,000 subscribers	MX240, MX480, MX960	S-SA-UP-256K

Software Feature Licenses for SRX Series Devices

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 32](#) describes the Junos OS features that require licenses.

Table 32: Junos OS Feature Licenses

Junos OS License Requirements			
Feature	SRX550M	SRX1500	SRX5000 line
Access Manager	X		
BGP Route Reflectors			
Dynamic VPN	X		
IDP Signature Update*	X	X	X
Application Signature Update (Application Identification)*	X		X

Table 32: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements			
Feature	SRX550M	SRX1500	SRX5000 line
Juniper-Kaspersky Antivirus*	X		
Juniper-Sophos Antivirus*	X	X	X
Juniper-Sophos Antispam*	X	X	X
Juniper-Enhanced Web filtering*	X	X	X
Juniper-Websense Web filtering*	X		
Logical Systems			X
UTM	X	X	X

* Indicates support on high-memory devices only.

Table 33 lists the licenses you can purchase for each SRX Series software feature. Each license allows you to run the specified advanced software features on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 33: Junos OS Feature License Model Number for SRX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Application Security and IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-APPSEC-A-1
		SRX550-APPSEC-A-3
		SRX550-APPSEC-A-5
	SRX5400	SRX5400-APPSEC-1
		SRX5400-APPSEC-3
		SRX5400-APPSEC-5
	SRX5600	SRX5600-APPSEC-A-1
		SRX5600-APPSEC-A-3
		SRX5600-APPSEC-A-5
	SRX5800	SRX5800-APPSEC-A-1
		SRX5800-APPSEC-A-3
		SRX5800-APPSEC-A-5
IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-IDP
		SRX550-IDP-3
		SRX550-IDP-5
IDP subscription (1 year and 3 years)	SRX1500	SRX1500-IPS-1
		SRX1500-IPS-3
	SRX5400, SRX5600, SRX5800	SRX5K-IDP
		SRX5K-IDP-3
		SRX5K-IDP-3-R
		SRX5K-IDP-R
Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-K-AV
		SRX550-K-AV-3
		SRX550-K-AV-5
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S-AV
		SRX550-S-AV-3
		SRX550-S-AV-5

Table 33: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antivirus updates (1 year)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S2-AS
		SRX550-S2-AS-3
		SRX550-S2-AS-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX550	SRX550-W-EWF
		SRX550-W-EWF-3
		SRX550-W-EWF-5
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX5400	SRX5400-W-EWF-1
		SRX5400-W-EWF-3
		SRX5400-W-EWF-5
Juniper-Enhanced Web filtering (1 year)	SRX5600	SRX5600-W-EWF-1
	SRX5800	SRX5800-W-EWF-1
Enterprise Bundle—Kaspersky Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-SMB4-CS
		SRX550-SMB4-CS-3
		SRX550-SMB4-CS-5

Table 33: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-S-SMB4- CS
		SRX550-S-SMB4- CS-3
		SRX550-S-SMB4- CS-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years)	SRX1500	SRX1500-CS-BUN-1
		SRX1500-CS-BUN-3
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX5400	SRX5400-CS-BUN-1
		SRX5400-CS-BUN-3
		SRX5400-CS-BUN-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year)	SRX5600	SRX5600-CS-BUN-1
	SRX5800	SRX5800-CS-BUN-1
Dynamic VPN Client (5, 10, and 25 simultaneous users)	SRX550	SRX-RAC-5-LTU
		SRX-RAC-10-LTU
		SRX-RAC-25-LTU
Dynamic VPN Service (5, 10, 25, and 50 simultaneous users)	SRX550	SRX-RAC-5-LTU
	SRX550	SRX-RAC-10-LTU
	SRX550	SRX-RAC-25-LTU
	SRX550	SRX-RAC-50-LTU
Dynamic VPN Service (100 and 150 simultaneous users)	SRX550	SRX-RAC-100-LTU
		SRX-RAC-150-LTU
Dynamic VPN Service (250 simultaneous users)	SRX550 <i>NOTE:</i> Requires Junos OS 11.2R3 or later	SRX-RAC-250-LTU
Dynamic VPN Service (500 simultaneous users)	SRX550 <i>NOTE:</i> Requires Junos OS 11.2R3 or later	SRX-RAC-500-LTU

Table 33: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Express Path License (formerly known as <i>services offloading</i>)	SRX5400, SRX5600, SRX5800	SRX5K-SVCS-OFFLOAD-RTU
<p>NOTE: Prior to Junos OS Release 12.3X48-D10, Express Path was a licensed software feature. Starting with Junos OS Release 12.3X48-D10, the Express Path license is no longer required to enable this functionality. Your previously acquired Express Path license will not be effective anymore.</p>		
Logical Systems License (incremental 1, 5, and 25 numbers)	SRX5400	SRX-5400-LSYS-1
		SRX-5400-LSYS-5
		SRX-5400-LSYS-25
	SRX5600	SRX-5600-LSYS-1
		SRX-5600-LSYS-5
		SRX-5600-LSYS-25
	SRX5800	SRX-5800-LSYS-1
		SRX-5800-LSYS-5
		SRX-5800-LSYS-25
Sky Advanced Threat protection (1 year, 3 years)	SRX1500	SRX1500-ATP-1
		SRX1500-ATP-3
Command and Control feeds (1 year, 3 years)	SRX1500	SPOT-CC-1500-1Y
		SPOT-CC-1500-3Y

Software Features That Require Licenses on EX Series Switches

The following Junos OS features require an Enhanced Feature License (EFL) or Advanced Feature License (AFL) on EX Series devices:

- (EX2200 only) Bidirectional forwarding detection (BFD)
- (EX2200 only) Connectivity fault management (IEEE 802.lag)
- (EX2200 only) Internet Group Management Protocol version 1 (IGMPv1), IGMPv2, and IGMPv3

- (EX2200 and EX3300) OSPFv1/v2 (with 4 active interfaces)
- (EX2200 only) Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- (EX2200 and EX3300) Q-in-Q tunneling (IEEE 802.1ad)
- (EX2200 only) Real-time performance monitoring (RPM)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) Intermediate System-to-Intermediate System (IS-IS)
- (EX3200, EX4200, EX4500, EX6200, and EX8200) IPv6 protocols: OSPFv3, PIPng, IS-IS for IPv6, IPv6 BGP
- (EX3200, EX4200, EX4500, EX6200, and EX8200) MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs)

Table 34 lists the licenses you can purchase for each EX Series software feature. Each license allows you to run the specified enhanced software features on a single device.



NOTE:

For a Virtual Chassis deployment, two license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role:

- In an EX8200 Virtual Chassis, the devices in the master and backup roles are always XRE200 External Routing Engines.
- In all other Virtual Chassis, the devices in the master and backup roles are switches.

You do not need additional license keys for Virtual Chassis member switches that are in the licensed role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

For more details regarding EX Series feature licenses, see “[Understanding Software Licenses for EX Series Switches](#)” on page 246.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 34: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Enhanced Feature License for EX 2200-24T/P	EX2200	EX-24-EFL
Enhanced Feature License for EX 2200-48T/P	EX2200	EX-48-EFL

Table 34: Junos OS Enhanced Feature License (EFL) and Advanced Feature License (AFL) Model Number for EX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Enhanced Feature License for EX2200-C	EX2200-C	EX-12-EFL
Advanced Feature License for EX 3200-24T/P and EX 4200-24T/P/F/PX	EX3200, EX4200	EX-24-AFL
Advanced Feature License for EX 3200-48T/P, EX 4200-48T/P/F/PX, and EX4500-40F	EX3200, EX4200, EX4500	EX-48-AFL
Advanced Feature License for EX6200	EX6200	EX6200-AFL
XRE200 Advanced Feature License for EX8200	EX8200	EX-XRE200-AFL
Advanced Feature License for EX8208	EX8208	EX8208-AFL
Advanced Feature License for EX8216	EX8216	EX8216-AFL

Software Features That Require Licenses on the QFX Series



NOTE: If you try to configure a feature that is not licensed, you will receive syslog messages saying that you are using a feature that is licensable and that you do not possess a license for the feature. If you try to commit configuration changes for a feature that is not licensed, you will receive a commit warning saying that you have exceeded the allowed license limit for the feature.



NOTE: Virtual Extensible Local Area Network (VXLAN) is not supported on QFX3500 and QFX3600 devices. When you issue the `show licenses` command, you will see VXLAN in the CLI output, but the feature is not enabled.



NOTE: There is no separate license for Virtual Chassis like there is for Virtual Chassis Fabric.

Table 35 lists the standard Junos OS features licenses and supported QFX Series devices. For information on disaggregated Junos OS feature licenses, see *Disaggregated Software Features That Require Licenses on the QFX Series*.

For information about how to purchase a software license, contact your Juniper Networks sales representative.

Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series premium feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch	One per switch	QFX10002-36Q-PFL
	QFX10002-72Q switch		QFX10002-72Q-PFL
	QFX10008 switch		QFX10008-PFL
	QFX10016 switch		QFX10016-PFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX10002-36Q switch	One per switch	QFX10002-36Q-AFL
	QFX10002-72Q switch		QFX10002-72Q-AFL
	QFX10008 switch		QFX10008-AFL
	QFX10016 switch		QFX10016-AFL
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN), and Open vSwitch Database (OVSDB)	QFX3500, QFX3600, QFX5100-48S, and QFX5100-48T switches	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX-JSL-EDGE-ADV1
QFX Series advanced feature license for Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Multi-protocol Label Switching (MPLS), and Virtual Extensible Local Area Network (VXLAN) and Open vSwitch Database (OVSDB)	QFX5100-24Q and QFX5100-96S switches	One per switch, two per Virtual Chassis, and two per Virtual Chassis Fabric	QFX5100-HDNSE-LIC

Table 35: Standard Junos OS Feature Licenses and Model Numbers for QFX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Number of Licenses Required	Model Number
QFX Series advanced feature license for Border Gateway Protocol (BGP)	QFX3100 Director device	One per Node device in a network Node group	QFX-JSL-DRCTR-ADV1
QFX Series advanced feature license for Fibre Channel	QFX3500 switch	One per switch on which fibre channel ports are configured	QFX-JSL-EDGE-FC
QFX Series advanced feature license for Fibre Channel	QFX3100 Director device	One per QFX3500 Node device on which fibre channel ports are configured	QFX-JSL-DRCTR-FC
QFX Series advanced feature license for Fibre Channel - Capacity 16	QFX3100 Director device	One for up to 16 QFX3500 Node devices on which fibre channel ports are configured	QFX-JSL-DRCTR-FC-C16
QFX Series feature license for enabling fabric mode	QFX3500 and QFX3600 device	One per device	QFX3000-JSL-EDGE-FAB
QFX Series feature license for base software for QFX3000-G QFabric system	QFX3100 Director device	One per QFX3000-G QFabric system	QFX3008-JSL-DRCTR-FAB
QFX Series feature license for base software for QFX3000-M QFabric system	QFX3100 Director device	One per QFX3000-M QFabric system	QFX3000M-JSL-DRCTR-FAB
QFX and EX Series feature license for enabling Media Access Control security (MACsec)	QFX switches that support MACsec. See <i>Understanding Media Access Control Security (MACsec)</i> .	One per switch, two per Virtual Chassis,	EX-QFX-MACSEC-AGG
Virtual Chassis Fabric (VCF)	All member devices in a Virtual Chassis Fabric (VCF)	Two per Virtual Chassis Fabric (VCF)	QFX-VCF-LIC

Understanding Software Licenses for EX Series Switches

To enable and use some of the Juniper Networks operating system (Junos OS) features, you must purchase, install, and manage separate software licenses. If the switch has the appropriate software license, you can configure and use these features.

The Junos OS feature license (that is, the purchased authorization code) is universal. However, to conform to Junos OS feature licensing requirements, you must install a unique license key (a combination of the authorization code and the switch's serial number) on each switch.

For a Virtual Chassis deployment, two license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role:

- In an EX8200 Virtual Chassis, the devices in the master and backup roles are always XRE200 External Routing Engines.
- In all other Virtual Chassis, the devices in the master and backup roles are switches.

You do not need additional license keys for Virtual Chassis member switches that are in the linecard role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

This topic describes:

- [Purchasing a Software Feature License on page 246](#)
- [Features Requiring a License on EX2200 Switches on page 247](#)
- [Features Requiring a License on EX2300 Switches on page 248](#)
- [Features Requiring a License on EX3300 Switches on page 248](#)
- [Features Requiring a License on EX3400 Switches on page 249](#)
- [Features Requiring a License on EX4300 Switches on page 250](#)
- [Features Requiring a License on EX4600 Switches on page 252](#)
- [Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches on page 253](#)
- [License Warning Messages on page 254](#)

Purchasing a Software Feature License

The following sections list features that require separate licenses. To purchase a software license, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.



NOTE: You are required to provide the 12-digit serial number when purchasing a license for an XRE200 External Routing Engine in an EX8200 Virtual Chassis.

The serial number listed on the XRE200 External Routing Engine serial ID label is 16 digits long. Use the last 12 digits of the 16-digit serial number to purchase the license.

You can use the `show chassis hardware` command output to display the 12-digit serial number of the XRE200 External Routing Engine.

Features Requiring a License on EX2200 Switches

For EX2200 switches, the following features can be added to basic Junos OS by installing an enhanced feature license (EFL):

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- OSPFv1/v2 (with four active interfaces)
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 36 lists the EFLs that you can purchase for EX2200 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2200 switch.

Table 36: Junos OS EFL Part Number on EX2200 Switches

Switch Model	EFL Part Number
EX2200-C-12P-2G EX2200-C-12T-2G	EX-12-EFL
EX2200-24T-4G EX2200-24P-4G EX2200-24T-DC-4G	EX-24-EFL
EX2200-48T-4G EX2200-48P-4G	EX-48-EFL

Features Requiring a License on EX2300 Switches

EX2300 switches has an enhanced feature licenses (EFLs).

To use the following features on the EX2300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6
- Multicast Source Discovery protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng
- Virtual Router Redundancy Protocol (VRRP)

[Table 37](#) lists the EFLs that you can purchase for EX2300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2300 switch.

Table 37: Junos OS EFL Part Number on EX2300 Switches

Switch Model	EFL Part Number
EX2300-24T EX2300-24P EX2300-C-12P EX2300-C-12T	EX-24-EFL

Features Requiring a License on EX3300 Switches

Two types of licenses are available on EX3300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX3300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6, virtual router support for unicast and filter-based forwarding (FBF)
- OSPFv1/v2

- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 38 lists the EFLs that you can purchase for EX3300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3300 switch.

Table 38: Junos OS EFL Part Number on EX3300 Switches

Switch Model	EFL Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-EFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-EFL

To use the following feature on EX3300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- IPv6 routing protocols: IPv6 BGP and IPv6 for MBGP
- Virtual routing and forwarding (VRF) BGP

Table 39 lists the AFLs that you can purchase for EX3300 switch models. For EX3300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX3300 switch.

Table 39: Junos OS AFL Part Number on EX3300 Switches

Switch Model	AFL Part Number
EX3300-24T EX3300-24P EX3300-24T-DC	EX-24-AFL
EX3300-48T EX3300-48T-BF EX3300-48P	EX-48-AFL

Features Requiring a License on EX3400 Switches

EX3400 switches has an enhanced feature licenses (EFLs) and MACSec license.

To use the following features on the EX3400 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols : Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6, virtual router support for unicast and filter-based forwarding (FBF)
- Multicast Source Discovery Protocol (MSDP)
- OSPF v2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 40 lists the EFLs that you can purchase for EX3400 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3400 switch.

Table 40: Junos OS EFL Part Number on EX3400 Switches

Switch Model	EFL Part Number
EX3400-24T EX3400-24P	EX-24-EFL
EX3400-48T EX3400-48P EX3400-48T-AFI	EX-48-EFL

Features Requiring a License on EX4300 Switches

Two types of licenses are available on EX4300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX4300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- Multicast Source Discovery Protocol (MSDP)
- OSPFv2/v3

- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng (RIP next generation)
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 41 lists the EFLs that you can purchase for EX4300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX4300 switch.

Table 41: Junos OS EFL Part Number on EX4300 Switches

Switch Model	EFL Part Number
EX4300-24T EX4300-24P	EX4300-24-EFL
EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-EFL
EX4300-32F EX4300-32F-DC	EX4300-32F-EFL

To use the following features on EX4300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)

Table 42 lists the AFLs that you can purchase for EX4300 switch models. For EX4300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX4300 switch.

Table 42: Junos OS AFL Part Number on EX4300 Switches

Switch Model	AFL Part Number
EX4300-24T EX4300-24P	EX4300-24-AFL
EX4300-48P EX4300-48T EX4300-48T-AFI EX4300-48T-DC EX4300-48T-DC-AFI	EX4300-48-AFL

Table 42: Junos OS AFL Part Number on EX4300 Switches (*continued*)

Switch Model	AFL Part Number
EX4300-32F EX4300-32F-DC	EX4300-32F-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4300 switches.

Features Requiring a License on EX4600 Switches

To use the following features on EX4600 switches, you must install an advanced feature license:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)
- Multiprotocol Label Switching (MPLS)

Table 43 lists the AFLs that you can purchase for EX4600 switch models.

Table 43: Junos OS AFL Part Number on EX4600 Switches

Switch Model	AFL Part Number
EX4600-40F	EX4600-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4600 switches.

Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches

To use the following features on EX3200, EX4200, EX4500, EX4550, EX8200, and EX9200 switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Ethernet VPN (available only on EX9200 switches)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP, IPv6 for MBGP
- Logical systems (available only on EX9200 switches)
- MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCCs) (Not supported on EX9200 switches)
- Open vSwitch Database (OVSDb) (available only on EX9200 switches)
- Virtual Extensible LAN (VXLAN) (available only on EX9200 switches)

To use the following features on Juniper Networks EX6200 Ethernet Switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP

Table 34 lists the AFLs that you can purchase for EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 switches. If you have the license, you can run all of the advanced software features mentioned above on your EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, or EX9200 switch.

Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches

Switch Model	AFL Part Number
EX3200-24P EX3200-24T EX4200-24F EX4200-24P EX4200-24PX EX4200-24T	EX-24-AFL
EX3200-48P EX3200-48T EX4200-48F EX4200-48P EX4200-48PX EX4200-48T	EX-48-AFL

Table 44: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches (*continued*)

Switch Model	AFL Part Number
EX4500-40F-BF EX4500-40F-BF-C EX4500-40F-FB EX4500-40F-FB-C	EX-48-AFL
EX4550	EX4550-AFL
EX6210	EX6210-AFL
EX8208	EX8208-AFL
EX8216	EX8216-AFL
EX-XRE200	EX-XRE200-AFL
EX9204	EX9204-AFL
EX9208	EX9208-AFL
EX9214	EX9214-AFL

You must download a MACsec feature license to enable MACsec. The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series switches cannot be purchased to enable MACsec.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key.

MACsec is supported on EX4200 and EX4550 switches.

License Warning Messages

For using features that require a license, you must install and configure a license key. To obtain a license key, use the contact information provided in your certificate.

If you have not purchased the AFL or EFL and installed the license key, you receive warnings when you try to commit the configuration:

```
[edit protocols]
  'bgp'
    warning: requires 'bgp' license
error: commit failed: (statements constraint check failed)
```

The system generates system log (**syslog**) alarm messages notifying you that the feature requires a license—for example:

```
Sep 3 05:59:11 craftd[806]: Minor alarm set, BGP Routing Protocol usage
requires a license
Sep 3 05:59:11 alarmd[805]: Alarm set: License color=YELLOW, class=CHASSIS,
reason=BGP Routing Protocol usage requires a license
Sep 3 05:59:11 alarmd[805]: LICENSE_EXPIRED: License for feature bgp(47) expired
```

Output of the **show system alarms** command displays the active alarms:

```
user@switch> show system alarms
1 alarm currently active
Alarm time          Class  Description
2009-09-03 06:00:11 UTC  Minor  BGP Routing Protocol usage requires a license
```

**Related
Documentation**

- *Managing Licenses for the EX Series Switch (CLI Procedure)*
- *Managing Licenses for the EX Series Switch (J-Web Procedure)*
- *Monitoring Licenses for the EX Series Switch*
- *License Key Components for the EX Series Switch*

Installing and Managing Licenses

- [Adding New Licenses \(CLI Procedure\) on page 257](#)
- [Deleting a License \(CLI Procedure\) on page 258](#)
- [Saving License Keys on page 259](#)
- [Verifying Junos OS License Installation on page 260](#)

Adding New Licenses (CLI Procedure)

Before adding new licenses, complete the following tasks:

- Purchase the required licenses.
- Establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your device.



NOTE: On QFabric systems, install your licenses in the default partition of the QFabric system and not on the individual components (Node devices and Interconnect devices).

To add a new license key to the device using the CLI:

1. From the CLI operational mode, enter one of the following CLI commands:

- To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

```
user@host> request system license add filename | url
```

- To add a license key from the terminal, enter the following command:

```
user@host> request system license add terminal
```

2. When prompted, enter the license key, separating multiple license keys with a blank line.

If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit license entry mode.

3. Go on to [“Verifying Junos OS License Installation” on page 260](#).

On routers that have graceful Routing Engine switchover (GRES) enabled, after successfully adding the new license on the master Routing Engine, the license keys are automatically synchronized on the backup Routing Engine as well. However, in case GRES is not enabled, the new license is added on each Routing Engine separately. This ensures that the license key is enabled on the backup Routing Engine during changeover of mastership between the Routing Engines.

To add a new license key to a router with dual Routing Engines without GRES:

1. After adding the new license key on the master Routing Engine, use the **request chassis routing-engine master switch** command to have the backup Routing Engine become the master Routing Engine.
2. Log in to the active Routing Engine and add the new license key, repeat the same step.



NOTE: Adding a license key to the router or switch might be delayed if a kernel resynchronization operation is in progress at that time. The following message is displayed on the CLI when the license-adding operation is about to be delayed:

A kernel re-sync operation is in progress. License update may take several minutes to complete.

Related Documentation

- [Deleting a License \(CLI Procedure\) on page 258](#)
- [Junos OS Feature Licenses on page 223](#)
- [Verifying Junos OS License Installation on page 260](#)
- [request system license add on page 302](#)

Deleting a License (CLI Procedure)

Before deleting a license, establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your router or switch.

You have the options to delete a single license, delete all licenses, or delete a list of licenses enclosed in brackets.

1. Display the licenses available to be deleted.

```
user@host> request system license delete license-identifier-list ?
```

Possible completions:

E00468XXX4	License key identifier
JUNOS10XXX1	License key identifier
JUNOS10XXX2	License key identifier
JUNOS10XXX3	License key identifier
JUNOS10XXX4	License key identifier
[Open a set of values

2. To delete a license key or keys from a device using the CLI operational mode, select one of the following methods:

- Delete a single license by specifying the license ID. Using this option, you can delete only one license at a time.

```
user@host> request system license delete license-identifier
```

- Delete all license keys from the current device.

```
user@host> request system license delete all
```

- Delete multiple license keys from the current device. Specify the license identifier for each key and enclose the list of identifiers in brackets.

```
user@host> request system license delete license-identifier-list [JUNOS10XXX1  
JUNOS10XXX3 JUNOS10XXX4 ...]
```

```
Delete license(s) ?  
[yes,no] (no) yes
```

3. Go on to “[Verifying Junos OS License Installation](#)” on page 260.



NOTE: Deleting a license key from the router or switch might be delayed if a kernel resynchronization operation is in progress at that time. The following message is displayed on the CLI when the license-deleting operation is about to be delayed:

A kernel re-sync operation is in progress. License update may take several minutes to complete.

Related Documentation

- [Adding New Licenses \(CLI Procedure\) on page 257](#)
- [Saving License Keys on page 259](#)
- [Junos OS Feature Licenses on page 223](#)
- [Verifying Junos OS License Installation on page 260](#)
- [request system license delete on page 303](#)

Saving License Keys

Before saving a license, establish basic network connectivity with the router or switch. For instructions on establishing basic connectivity, see the *Getting Started Guide* or *Quick Start Guide* for your router or switch.

To save the licenses installed on a device to a file using the CLI:

1. From the CLI operational mode, enter one of the following CLI commands:

- To save the installed license keys to a file or URL, enter the following command:

```
user@host> request system license save filename | url
```

For example, the following command saves the installed license keys to a file named **license.config**:

- To save a license key from the terminal, enter the following command:

```
user@host> request system license save ftp://user@host/license.config
```

2. Go on to “Verifying Junos OS License Installation” on page 260.

Related Documentation

- [Adding New Licenses \(CLI Procedure\) on page 257](#)
- [Deleting a License \(CLI Procedure\) on page 258](#)
- [Junos OS Feature Licenses on page 223](#)
- [Verifying Junos OS License Installation on page 260](#)

Verifying Junos OS License Installation

To verify Junos OS license management, perform the following tasks:

- [Displaying Installed Licenses on page 260](#)
- [Displaying License Usage on page 261](#)

Displaying Installed Licenses

Purpose Verify that the expected licenses are installed and active on the router or switch.

Action From the CLI, enter the **show system license** command.

Sample Output

```
user@host> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
subscriber-acct	0	1	0	permanent
subscriber-auth	0	1	0	permanent
subscriber-addr	0	1	0	permanent
subscriber-vlan	0	1	0	permanent
subscriber-ip	0	1	0	permanent
scale-subscriber	0	1000	0	permanent
scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent

Licenses installed:

License identifier: E000185416

License version: 2

Features:

```
subscriber-acct - Per Subscriber Radius Accounting
permanent
subscriber-auth - Per Subscriber Radius Authentication
permanent
subscriber-addr - Address Pool Assignment
permanent
subscriber-vlan - Dynamic Auto-sensed Vlan
permanent
subscriber-ip   - Dynamic and Static IP
permanent
```

Meaning The output shows a list of the license usage and a list of the licenses installed on the router or switch. Verify the following information:

- Each license is present. Licenses are listed in ascending alphanumeric order by license ID.
- The state of each license is **permanent**.



NOTE: A state of invalid indicates that the license key is not a valid license key. Either it was entered incorrectly or it is not valid for the specific device.

- The feature for each license is the expected feature. The features enabled are listed by license. An all-inclusive license has all features listed.
- All configured features have the required licenses installed. The Licenses needed column must show that no licenses are required.

Displaying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the router or switch.

Action From the CLI, enter the **show system license usage** command.

Sample Output

```
user@host> show system license usage
```

	Licenses used	Licenses installed	Licenses needed	Expiry
Feature name				
subscriber-addr	1	0	1	29 days
scale-subscriber	0	1000	0	permanent
scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent

Meaning The output shows any licenses installed on the router or switch and how they are used. Verify the following information:

- Any configured licenses appear in the output. The output lists features in ascending alphabetical order by license name. The number of licenses appears in the third column. Verify that you have installed the appropriate number of licenses.
- The number of licenses used matches the number of configured features. If a licensed feature is configured, the feature is considered used. The sample output shows that the subscriber address pooling feature is configured.
- A license is installed on the router or switch for each configured feature. For every feature configured that does not have a license, one license is needed.

For example, the sample output shows that the subscriber address feature is configured but that the license for the feature has not yet been installed. The license must be installed within the remaining grace period to be in compliance.

PART 4

Troubleshooting Information

- [Troubleshooting Software Installation on page 265](#)

CHAPTER 16

Troubleshooting Software Installation

- [Troubleshooting Software Installation on page 265](#)
- [Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 268](#)
- [Disk Space Management for Junos OS Installation on page 269](#)
- [Verifying PIC Combinations on page 269](#)

Troubleshooting Software Installation

This topic describes troubleshooting issues with software installations on EX Series switches.

- [Recovering from a Failed Software Upgrade on an EX Series Switch on page 265](#)
- [Rebooting from the Inactive Partition on page 266](#)
- [Freeing Disk Space for Software Installation on page 267](#)
- [Installation from the Boot Loader Generates 'cannot open package' Error on page 267](#)

Recovering from a Failed Software Upgrade on an EX Series Switch

Problem **Description:** If Junos OS loads but the CLI is not working, or if the switch has no software installed, use this recovery installation procedure to install Junos OS.

Solution If there is already a Junos OS image on the system, you can either install the new Junos OS package in a separate partition and have both Junos OS images remain on the system, or you can wipe the disk clean before the new installation proceeds.

If there is no Junos OS image on the system, follow the instructions in "[Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive](#)" on page 162 to get an image on the system and boot the switch.

To perform a recovery installation:

1. Power on the switch. The loader script starts.

After the message **Loading /boot/defaults/loader.conf** displays, you are prompted with:

Hit [Enter] to boot immediately, or space bar for command prompt.
2. Press the space bar to enter the manual loader. The **loader>** prompt displays.

3. Enter the following command:

```
loader> install [--format] [--external] source
```

where:

- **format**—Use this option to wipe the installation media before installing the software package. If you do not include this option, the system installs the new Junos OS package in a different partition from the partition used by the most recently installed Junos OS package.
- **external**—Use this option to install the software package on an external medium.
- **source**—Represents the name and location of the Junos OS package either on a server on the network or as a file on the USB flash drive:
 - Network address of the server and the path on the server; for example, **tftp://192.171.28/junos/jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**
 - The Junos OS package on a USB device is commonly stored in the root drive as the only file; for example, **file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz**

The boot process proceeds as normal and ends with a login prompt.

Rebooting from the Inactive Partition

Problem **Description:** EX Series switches shipped with Junos OS Release 10.4R2 or earlier have Junos OS loaded on the system disk in partition 1. The first time you upgrade, the new software package is installed in partition 2. When you finish the installation and reboot, partition 2 becomes the active partition. Similarly, subsequent software packages are installed in the inactive partition, which becomes the active partition when you reboot at the end of the installation process.

On switches shipped with Release 10.4R3 and later, the same Junos OS image is loaded in each of the two root partitions, and you should copy the new software image to the alternate partition each time you upgrade.

If you performed an upgrade and rebooted, the system resets the active partition. You can use this procedure to manually boot from the inactive partition.



NOTE: If you have completed the installation of the software image but have not yet rebooted, issue the **request system software rollback** command to return to the original software installation package.

Solution Reboot from the inactive partition:

```
user@switch> request system reboot slice alternate
```



NOTE: If you cannot access the CLI, you can reboot from the inactive partition using the following procedure from the loader script prompt:

1. Unload and clear the interrupted boot from the active partition:

```
loader> unload
loader> unset vfs.root.mountfrom
```

2. Select the new (inactive) partition to boot from:

```
loader> set currdev=diskxsy:
```

where *x* is either 0 (internal) or 1 (external) and the *y* indicates the number of the inactive partition, either 1 or 2.

You must include the colon (:) at the end of this command.

3. Boot Junos OS from the inactive partition:

```
loader> boot
```

Freeing Disk Space for Software Installation

Problem **Description:** The software installation process requires a certain amount of unused disk space. If there is not enough space, you might receive an error message such as:

```
fetch: /var/tmp/incoming-package.tgz: No space left on device
```

Solution Identify and delete unnecessary files by using the [request system storage cleanup](#) command.

Installation from the Boot Loader Generates 'cannot open package' Error

Problem **Description:** When installing a Junos OS software image from the loader prompt, a "cannot open package error" is generated:

```
loader> install - -format
tftp://10.204.33.248/images/Flash_corr/official/jinstall-ex-4200-10.4I2011012-domestic-signed.tgz
Speed: 1000, full duplex
bootp: no reply
No response for RARP request
net_open: RARP failed
cannot open package (error 5)
```

Solution This might be due to the IP address, gateway IP address, netmask address, or server IP address not being properly set. You can set these values either from the shell or from the u-boot prompt.

To set these values from the shell:

```
% nvram setenv ipaddr 10.204.35.235
% nvram setenv netmask 255.255.240.0
```

```
% nvram setenv gatewayip 10.204.47.254
% nvram setenv serverip 10.204.33.248
```

To set these values from the u-boot prompt, log in to a console connection, reboot, and stop at the u-boot prompt (Cntrl+c):

```
=> setenv ipaddr 10.204.35.235
=> setenv gatewayip 10.204.47.254
=> setenv serverip 10.204.33.248
=> setenv netmask 255.255.240.0
=> saveenv
=> printenv Verify whether variables are set properly or not
=> boot
```

Related Documentation

- *Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)*
- *Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)*
- [Installing Software on EX Series Switches \(J-Web Procedure\) on page 64](#)
- [Understanding Software Installation on EX Series Switches on page 44](#)
- [show system storage partitions \(EX Series Switches Only\) on page 415](#)

Troubleshooting a Switch That Has Booted from the Backup Junos OS Image

Problem **Description:** The switch boots from the backup root file partition. It is possible that the primary copy of JUNOS OS failed to boot properly, which could indicate that it is corrupted. This event is flagged in two ways:

- Upon login through the console or management port, the following warning message is displayed:

```
WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE
```

It is possible that the primary copy of JUNOS failed to boot up properly, and so this device has booted from the backup copy.

Please re-install JUNOS to recover the primary copy in case it has been corrupted.

- The following alarm message is generated:

```
user@switch> show chassis alarms
1 alarms currently active
Alarm time          Class  Description
2011-02-17 05:48:49 PST  Minor  Host 0 Boot from backup root
```

If the switch is in a Virtual Chassis, the switch member number appears in the **Description** field, where the switch is called a host.

Solution Install a new Junos OS image on the partition that had the corruption, or take a snapshot (use [request system snapshot](#)) of the currently active partition and use it to replace the image in the alternate partition:

If the switch is a standalone switch or a Virtual Chassis master switch, enter this command:

```
user@switch> request system snapshot slice alternate
```

If the switch is a Virtual Chassis member switch (not the master), enter this command on the Virtual Chassis:

```
user@switch> request system snapshot slice alternate member member-id
```

where *member-id* is the Virtual Chassis member ID number.

Related Documentation

- [Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131](#)
- [Troubleshooting Software Installation on page 265](#)
- [show system storage partitions \(EX Series Switches Only\) on page 415](#)

Disk Space Management for Junos OS Installation

A Junos OS installation or upgrade may fail if your router has a shortage of disk space. If a disk space error occurs, use one or more of the following options to complete the installation:

- Use the **request system storage cleanup** command to delete unnecessary files and increase storage space on the router.
- Specify the **unlink** option when you use the **request system software add** command to install the Junos OS:
 - On the M Series, MX Series, and T Series routers, the **unlink** option removes the software package after a successful upgrade.
- Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. The download program provides intelligent disk space management to enable installation.

Related Documentation

- [Junos OS Configuration Using the CLI](#)

Verifying PIC Combinations

SRX5600 and SRX5800 devices support IOC or SPC on any given card slot, and there is no complexity in equipping the services gateways with the perfect balance of processing and I/O capacity. You can install up to 11 (on SRX5800) and five (SRX5600) SPCs and IOCs on the device. However you must install at least one SPC on device. For more details, see [SRX5600 and SRX5800 Services Gateway Card Guide](#).

For more information about PIC combinations or about unsupported PIC combinations, see the corresponding PIC guide or *Hardware Guide* for your device, and the *Junos OS Release Notes* on the Juniper Networks Support website at <http://www.juniper.net/support/>.

- Related Documentation**
- [Hardware Overview of SRX Series Services Gateways on page 31](#)
 - [Storage Media Names for SRX Series Devices on page 34](#)

PART 5

Configuration Statements and Operational Commands

- [Configuration Statements on page 273](#)
- [Operational Commands on page 289](#)

CHAPTER 17

Configuration Statements

- [auto-configuration on page 274](#)
- [auto-configuration \(System\) on page 275](#)
- [auto-image-upgrade on page 277](#)
- [auto-snapshot on page 278](#)
- [autoinstallation on page 279](#)
- [autoinstallation \(JNU Satellite Devices\) on page 280](#)
- [bootp on page 281](#)
- [commit on page 282](#)
- [configuration-servers on page 283](#)
- [delete-after-commit \(JNU Satellites\) on page 284](#)
- [interfaces \(Autoinstallation\) on page 285](#)
- [license on page 286](#)
- [usb on page 288](#)
- [usb-control on page 288](#)

auto-configuration

Syntax	auto-configuration { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Configure the autoconfiguration process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the autoconfiguration process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Autoinstallation Overview on page 81• Configuring Autoinstallation on SRX Series Devices on page 84

auto-configuration (System)

Syntax	<pre> auto-configuration { traceoptions { file { filename; files number; match regular-expression; size maximum-file-size; (world-readable no-world-readable); } flag flag; level (all error info notice verbose warning); no-remote-trace; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the autoconfiguration process.
Options	<p>traceoptions—Set the trace options.</p> <ul style="list-style-type: none"> file—Configure the trace file information. <ul style="list-style-type: none"> filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced. files number—Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed to trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten. <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 files</p> <p>Default: 10 files</p> match regular-expression—Refine the output to include lines that contain the regular expression. size maximum-file-size—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
 - **all**—Trace all events.
 - **auth**—Trace VLAN authentication.
 - **configuration**—Trace configurations.
 - **interfaces**—Trace interface operations.
 - **io**—Trace I/O operations.
 - **rtsock**—Trace routing socket operations.
 - **ui**—Trace user interface operations.


Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Autoinstallation Overview on page 81• Configuring Autoinstallation on SRX Series Devices on page 84 |
|------------------------------|--|

auto-image-upgrade

Syntax	auto-image-upgrade;
Hierarchy Level	[edit chassis]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	<p>Enable automatic software download on an EX Series switch acting as a DHCP client.</p> <p>The DHCP client EX Series switch compares the software package name in the DHCP server message to the name of the software package that booted the switch. If the software packages are different, the DHCP client EX Series switch downloads and installs the software package specified in the DHCP server message.</p> <p>Before you upgrade software using automatic software download, ensure that you have configured DHCP services for the switch, including configuring a path to a boot server and a boot file. See the Junos OS System Basics Configuration Guide for information about using the CLI to configure DHCP services and settings. See <i>Configuring DHCP Services (J-Web Procedure)</i> for information about using the J-Web interface to configure DHCP services and settings.</p>
Default	Automatic software download is disabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Upgrading Software by Using Automatic Software Download on page 129 • Understanding Software Installation on EX Series Switches on page 44 • <i>Understanding DHCP Services for Switches</i>

auto-snapshot

Syntax	auto-snapshot;
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Enable the automatic snapshot feature, which allows the switch to automatically fix a corrupt Junos OS file in the primary root partition. If the automatic snapshot feature is enabled, the switch automatically takes a snapshot of the Junos OS root file system in the alternate root partition and copies it onto the primary root partition, thereby repairing the corrupt file in the primary root partition. The automatic snapshot procedure takes place whenever the system reboots from the alternate root partition, regardless of whether the reboot is due to a command or due to corruption of the primary root partition.
<div>  NOTE: EX9200 switches do not support the automatic snapshot feature. </div>	
Default	<ul style="list-style-type: none"> The automatic snapshot feature is enabled by default on the following EX Series switches: <ul style="list-style-type: none"> EX4550 switches EX Series switches that ship with Junos OS Release 12.3R1 or later The automatic snapshot feature is disabled by default on EX Series switches (except the EX4550 switches) running Junos OS Release 12.2 or earlier. If the automatic snapshot feature was disabled by default before the switch was upgraded to Junos OS Release 12.3R1 or later, the feature remains disabled (for backward compatibility) by default after the upgrade.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Understanding Resilient Dual-Root Partitions on Switches on page 95 show system auto-snapshot on page 394

autoinstallation

Syntax	<pre> autoinstallation { configuration-servers { url { password <i>password</i>; } } interfaces { <i>interface-name</i> { bootp; rarp; } } usb { disable; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the configuration for autoinstallation.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Autoinstallation on SRX Series Devices on page 84

autoinstallation (JNU Satellite Devices)

Syntax	<pre>autoinstallation { delete-after-commit; configuration-servers { url; } interfaces { interface-name { bootp; rarp; } } }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 13.3 for satellite devices in a Junos Node Unifier (JNU) group.
Description	(Satellite devices in a JNU group). Download a configuration file automatically from an FTP or HTTP server. When you power on a router or switch configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. When the router or switch has an address, it sends a request to a configuration server and downloads and installs a configuration.
Options	The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91• Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89• Configuring Autoinstallation on JNU Satellite Devices on page 87• Verifying Autoinstallation on JNU Satellite Devices on page 92• delete-after-commit (JNU Satellites) on page 284• configuration-servers

bootp

Syntax	<pre>bootp { command <i>binary-file-path</i>; disable; failover (alternate-media other-routing-engine); }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the booting process.
Options	<ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to the binary process. • disable —Disable the booting process. • failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot. <ul style="list-style-type: none"> • alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly. • other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> •

commit

Syntax

```
commit {  
  server {  
    commit-interval seconds;  
    days-to-keep-error-logs days;  
    maximum-aggregate-pool number;  
    maximum entries number;  
    traceoptions {  
      file {  
        filename;  
        files number;  
        microsecond-stamp;  
        size maximum-file-size;  
        (world-readable | no-world-readable);  
      }  
      flag flag;  
      no-remote-trace;  
    }  
  }  
  synchronize;  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 12.1.

Description Configure the commit operation.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Controlling Execution of Commit Scripts During Commit Operations*


configuration-servers

Syntax	<pre>configuration-servers { url { password <i>password</i>; } }</pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the URL address of a server from which the configuration files must be obtained.</p> <p>You can download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) servers. Examples of URLs:</p> <ul style="list-style-type: none"> • tftp://hostname/path/filename • ftp://username:password@ftp.hostname.net • http://hostname/path/filename • http://username:password@httpconfig.sp.com
Options	<ul style="list-style-type: none"> • url—Specify the URL address of the server containing the configuration files. • password—Specify the password for authentication with the configuration server. Specifying a password in URLs and in the <i>password</i> option might result in commit failure. We recommend you to use the <i>password</i> option for specifying the password.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Autoinstallation on SRX Series Devices on page 84

delete-after-commit (JNU Satellites)

Syntax	delete-after-commit;
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced in Junos OS Release 13.3 for satellite devices in a Junos Node Unifier (JNU) group.
Description	<p>Specify that during the subsequent commit operation of configuration settings (after the autoinstallation process successfully retrieves, installs, and commits the configuration), the autoinstallation configuration parameters be removed from the router. Removal of the autoinstallation parameters and statements from the committed configuration on the router ensures that the router does not attempt to perform an autoinstallation process when it is powered on the next time. Although you can optionally specify the interfaces to perform autoinstallation or configuration servers from which the files are to be downloaded, you must include the delete-after-commit statement to prevent the router from entering a recursive loop and repeatedly performing an autoinstallation every time it is powered on.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Autoinstallation of Satellite Devices in a Junos Node Unifier Group on page 91• Autoinstallation Process on Satellite Devices in a Junos Node Unifier Group on page 89• Configuring Autoinstallation on JNU Satellite Devices on page 87• Verifying Autoinstallation on JNU Satellite Devices on page 92• autoinstallation on page 280• configuration-servers

interfaces (Autoinstallation)

Syntax	<pre> interfaces { interface-name { bootp; rarp; } } </pre>
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.
<div>  <p>NOTE: When you run the <code>system autoinstallation</code> command, the command will configure unit 0 logical interface for all the active state physical interfaces. However, few commands like <code>fabric-options</code> do not allow its physical interface to be configured with a logical interface. If the <code>system autoinstallation</code> and the <code>fabric-options</code> commands are configured together the following message is displayed incompatible with 'system autoinstallation'.</p> </div>	
Options	<ul style="list-style-type: none"> • bootp—Enables BOOTP or DHCP during autoinstallation. • rarp—Enables RARP during autoinstallation.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Autoinstallation Overview on page 81 • Configuring Autoinstallation on SRX Series Devices on page 84

license

Syntax	<pre> license { autoupdate { url <i>url</i>; password <i>password</i>; } renew { before-expiration <i>number</i>; interval <i>interval-hours</i>; } traceoptions { file { <i>filename</i> ; files <i>number</i>; match <i>regular-expression</i>; size <i>maximum-file-size</i>; (world-readable no-world-readable); } flag <i>flag</i>; no-remote-trace; } } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify license information for the device.
Options	<ul style="list-style-type: none"> • autoupdate—Autoupdate license keys from license servers. <ul style="list-style-type: none"> • url—URL of a license server. • renew—License renewal lead time and checking interval. <ul style="list-style-type: none"> • before-expiration <i>number</i>—License renewal lead time before expiration in days. Range : 0 through 60 days • interval <i>interval-hours</i>—License checking interval in hours. Range : 1 through 336 hours • traceoptions—Set the trace options. <ul style="list-style-type: none"> • file—Configure the trace file information. <ul style="list-style-type: none"> • <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced. • files <i>number</i>— Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size *maximum file-size*** option.

Range : 2 through 1000 files

Default : 10 files

- **match *regular-expression***—Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Range : 10 KB through 1 GB

Default : 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files *number*** option.

- **(world-readable | no-world-readable)**— By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag *flag***—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
 - **all**—Trace all operations
 - **config**—Trace license configuration processing.
 - **events**—Trace licensing events and their processing.
 - **no-remote-trace**—Disable the remote tracing.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	• Junos OS Feature License Keys on page 1145
------------------------------	--

usb

Syntax	usb { disable; }
Hierarchy Level	[edit system autoinstallation]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Disable the USB autoinstallation process.
Options	disable —Disable the process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Autoinstallation on SRX Series Devices on page 84

usb-control

Syntax	usb-control { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the universal serial bus (USB) supervise process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the universal serial bus (USB) supervise process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

CHAPTER 18

Operational Commands


- clear system login lockout
- request system autorecovery state
- request system download abort
- request system download clear
- request system download pause
- request system download resume
- request system download start
- request system firmware upgrade
- request system halt
- request system license add
- request system license delete
- request system license save
- request system license update
- request system partition compact-flash
- request system power-off
- request system reboot
- request system reboot
- request system reboot (Junos OS with Upgraded FreeBSD)
- request system scripts add
- request system scripts delete
- request system scripts rollback
- request system snapshot
- request system snapshot (Junos OS with Upgraded FreeBSD)
- request system snapshot (SRX Series)
- request system software abort in-service-upgrade (ICU)
- request system software add
- request system software add (Maintenance)
- request system software configuration-backup

- `request system software configuration-restore`
- `request system software delete`
- `request system software rollback`
- `request system software rollback (SRX Series)`
- `request system software validate`
- `request system software validate on (Junos OS with Upgraded FreeBSD)`
- `request system storage cleanup`
- `request system storage cleanup (SRX Series)`
- `request system zeroize`
- `show chassis usb storage`
- `show system autoinstallation status`
- `show system autorecovery state`
- `show system boot-messages`
- `show system auto-snapshot`
- `show system download`
- `show system license`
- `show system license (View)`
- `show system login logout`
- `show system snapshot`
- `show system snapshot (Junos OS with Upgraded FreeBSD)`
- `show system snapshot media`
- `show system storage partitions (EX Series Switches Only)`
- `show system storage partitions (View SRX Series)`

clear system login logout

Syntax	clear system login logout <all> <user <i>username</i> >
Release Information	Command introduced in Junos OS Release 11.2.
Description	Unlock the user account locked as a result of invalid login attempts.
Options	all —Clear all locked user accounts. user <i>username</i> —Clear the specified locked user account.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• lockout-period on page 1244• show system login logout on page 409
Output Fields	This command produces no output.

request system autorecovery state

Syntax	request system autorecovery state (save recover clear)
Release Information	Command introduced in Junos OS Release 11.2.
Description	Prepare the system for autorecovery of configuration, licenses, and disk information.
Options	<p>save—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.</p> <p>The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.</p>
	<div>  <p>NOTE:</p> <ul style="list-style-type: none"> Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed. A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten. </div>
	<p>recover—Recover the disk partitioning, configuration, and licenses.</p> <p>After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.</p>
	<p>clear—Clear all saved autorecovery information.</p> <p>Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> show system autorecovery state on page 385
List of Sample Output	request system autorecovery state save on page 293 request system autorecovery state recover on page 293 request system autorecovery state clear on page 293
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving bsdlablel recovery information
```

Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover


Configuration:
File           Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File           Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Saved                Failed           Recovered
BSD Labels:
Slice          Recovery Information  Integrity Check  Action / Status
s1             Saved                Passed           None
s2             Saved                Passed           None
s3             Saved                Passed           None
s4             Saved                Passed           None
```

Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear
Clearing config recovery information
Clearing license recovery information
Clearing bsdlablel recovery information
```

request system download abort

Syntax	<code>request system download abort <download-id></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the show system download command until a request system download clear operation is performed.
<div> NOTE: Only downloads in the active, paused, and error states can be aborted.</div>	
Options	download-id —(Required) The ID number of the download to be aborted.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 298• request system download pause on page 296• request system download resume on page 297• request system download clear on page 295
List of Sample Output	request system download abort on page 294
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

request system download clear


Syntax	request system download clear
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Delete the history of completed and aborted downloads.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 298• request system download pause on page 296• request system download resume on page 297• request system download abort on page 294
List of Sample Output	request system download clear on page 295
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause


Syntax	request system download pause <download-id>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Suspend a particular download instance.
<div> NOTE: Only downloads in the active state can be paused.</div>	
Options	download-id —(Required) The ID number of the download to be paused.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 298• request system download resume on page 297• request system download abort on page 294• request system download clear on page 295
List of Sample Output	request system download pause on page 296
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```


request system download resume

Syntax	<code>request system download resume <i>download-id</i> <max-rate></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the request system download start command. The user can optionally specify a new (maximum) bandwidth with the request system download resume command.
<div>  NOTE: Only downloads in the paused and error states can be resumed. </div>	
Options	download-id —(Required) The ID number of the download to be resumed. max-rate —(Optional) The maximum bandwidth for the download.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 298 • request system download pause on page 296 • request system download abort on page 294 • request system download clear on page 295
List of Sample Output	request system download resume on page 297
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

Syntax	<code>request system download start (<i>url</i> <i>max-rate</i> <i>save as</i> <i>login</i> <i>delay</i>)</code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Creates a new download instance and identifies it with a unique integer called the download ID.
Options	<p>url—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p>max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.</p> <p>save-as—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p>login—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p>delay—(Optional) The number of hours after which the download should start.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download pause on page 296• request system download resume on page 297• request system download abort on page 294• request system download clear on page 295
List of Sample Output	request system download start on page 298
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server/tftpboot/1m_file
max-rate 1k
Starting download #1
```

request system firmware upgrade

Syntax	request system firmware upgrade
Release Information	Command introduced in Junos OS Release 10.2.
Description	Upgrade firmware on a system.
Options	<p>fpc—Upgrade FPC ROM monitor.</p> <p>pic—Upgrade PIC firmware.</p> <p>re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p>vcpu—Upgrade VCPU ROM monitor.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> request system license update on page 305
List of Sample Output	request system firmware upgrade on page 299
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```

user@host> request system firmware upgrade re bios
Part          Type          Tag Current  Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1 1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re bios backup
Part          Type          Tag Current  Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1 1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

```

request system halt

Syntax	<code>request system halt</code> <code>at <time></code> <code>both-routing-engines</code> <code>in <minutes></code> <code>media (compact-flash disk usb)</code> <code>messages <message></code> <code>other-routing-engine</code>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Stop the system.
Options	<p>at <i>time</i>— Time at which to stop the system.</p> <p>in <i>minutes</i>— Number of minutes to delay before halting the system.</p> <p>media —Boot media for the next boot.</p> <ul style="list-style-type: none">• compact-flash— Standard boot from a flash device.• disk— Boot from a hard disk.• usb— Boot from a USB device. <p>message <i>message</i>— Message that is displayed to all system users before stopping the system.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system power-off on page 307
List of Sample Output	request system halt on page 300
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system halt

```
user@host> request system halt
Halt the system ? [yes,no] (no) yes

*** FINAL System shutdown message from root@quickland ***

System going down IMMEDIATELY

Shutdown NOW!
[pid 7560]
```

```
root@quickland> Dec  8 08:57:37 Waiting (max 60 seconds) for system process `vnlru'
to stop...done
Waiting (max 60 seconds) for system process `vnlru_mem' to stop...done
Waiting (max 60 seconds) for system process `bufdaemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
Syncing disks, vnodes remaining...2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 0 0 0 0 0 0
0 0 0 0 0 done

syncing disks... All buffers synced.
Uptime: 2d16h25m9s
recorded reboot as normal shutdown

The operating system has halted.
Please press any key to reboot.
```

request system license add

Syntax	<code>request system license add (<i>filename</i> terminal)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 9.5 for SRX Series devices. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Add a license key.
Options	<i>filename</i> —License key from a file or URL. Specify the filename or the URL where the key is located. <i>terminal</i> —License key from the terminal.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Adding New Licenses (CLI Procedure) on page 257
List of Sample Output	request system license add on page 302
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license add

```
user@host> request system license add terminal
E408408918 aeaqib qcsbja okbuqe rcmxnq vjocwf uxfsta
          z5ufjb kdrmt6 57bimv 2f3ddp qttcdn 627q4a
          jx4s5x hiri
E408408918: successfully added
add license complete (no errors)
```

request system license delete

Syntax	<code>request system license delete (<i>license-identifier</i> license-identifier-list [<i>licenseid001</i> <i>licenseid002</i> <i>licenseid003</i>] all)</code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Option license-identifier-list introduced in Junos OS Release 13.1.</p>
Description	Delete a license key. You can choose to delete one license at a time, all licenses at once, or a list of license identifiers enclosed in brackets.
Options	<p>license-identifier—Text string that uniquely identifies a license key.</p> <p>license-identifier-list [<i>licenseid001</i> <i>licenseid002</i> <i>licenseid003</i>....]—Delete multiple license identifiers as a list enclosed in brackets.</p> <p>all—Delete all licenses on the device.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Deleting a License (CLI Procedure) on page 258

request system license save

Syntax	<code>request system license save (<i>filename</i> terminal)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 9.5 for SRX Series devices.
Description	Save installed license keys to a file or URL.
Options	<i>filename</i> —License key from a file or URL. Specify the filename or the URL where the key is located. <i>terminal</i> —License key from the terminal.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Saving License Keys on page 259
List of Sample Output	request system license save on page 304
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license save

```
user@host> request system license save ftp://user@host/license.conf
```


request system license update

Syntax	<code>request system license update</code>
Release Information	Command introduced in Junos OS Release 9.5.
Description	Start autoupdating license keys from the LMS server.
Options	<code>trial</code> —Starts autoupdating trial license keys from the LMS server.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • show system license (View) on page 406
List of Sample Output	request system license update on page 305 request system license update trial on page 305
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update
```


```
Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system partition compact-flash

Syntax	request system partition compact-flash
Release Information	Command introduced in Junos OS Release 9.2. Command deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.
<div>  NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “Understanding Junos OS with Upgraded FreeBSD” on page 19. </div>	
Description	Reboots the device and repartitions the compact flash. The CompactFlash card is repartitioned only if it is possible to restore all the data on the CompactFlash card. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.
Required Privilege Level	maintenance
List of Sample Output	request system partition compact-flash (If Yes) on page 306 request system partition compact-flash (If No) on page 306
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system partition compact-flash (If Yes)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>

```

Sample Output

request system partition compact-flash (If No)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no

```

request system power-off

Syntax	<pre>request system power-off at <time> both-routing-engines in <minutes> media (compact-flash disk usb) messages <message> other-routing-engine</pre>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Power off the system.
Options	<p>at <i>time</i>— Time at which to power off the system.</p> <p>both-routing-engines— Both routing engines are powered off and both the primary and the secondary devices are rebooted at the same time.</p> <p>in <i>minutes</i>— Number of minutes to delay before powering off the system.</p> <p>media —Boot media for the next boot.</p> <ul style="list-style-type: none"> • compact-flash— Standard boot from a flash device. • disk— Boot from a hard disk. • usb— Boot from a USB device. <p>message <i>message</i>— Message that is displayed to all system users before powering off the system.</p> <p>other-routing-engine— The other routing engine is powered off.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system halt on page 300
List of Sample Output	request system power-off on page 307
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system power-off

```
user@host> request system power-off
Power Off the system ? [yes,no] (no) yes

Shutdown NOW!
[pid 3300]
```

*** FINAL System shutdown message from root@quickland ***

System going down IMMEDIATELY

```
root@quickland> Dec  8 09:37:45 Waiting (max 60 seconds) for system process `vnlr'
to stop...done
Waiting (max 60 seconds) for system process `vnlr_mem' to stop...done
Waiting (max 60 seconds) for system process `bufdaemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
Syncing disks, vnodes remaining...2 2 2 2 2 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
0 0 0 0 done
```

```
syncing disks... All buffers synced.
Uptime: 38m33s
recorded reboot as normal shutdown
```

```
The operating system has halted.
Turning the system power off.
```

request system reboot

List of Syntax	Syntax on page 309 Syntax (EX Series Switches) on page 309 Syntax (TX Matrix Router) on page 309 Syntax (TX Matrix Plus Router) on page 309 Syntax (MX Series Router) on page 309
Syntax	<pre>request system reboot <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk removable-compact-flash usb)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (EX Series Switches)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local> <media (external internal)> <member <i>member-id</i>> <message "<i>text</i>"> <other-routing-engine> <slice <i>slice</i>></pre>
Syntax (TX Matrix Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> scc> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (TX Matrix Plus Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i>> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine> <partition (1 2 alternate)></pre>
Syntax (MX Series Router)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local></pre>

```
<media (external | internal)>
<member member-id>
<message "text">
<other-routing-engine>
```

Release Information Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

Description Reboot the software.

Options **none**—Reboot the software immediately.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.

at *time*—(Optional) Time at which to reboot the software, specified in one of the following ways:

- **now**—Stop or reboot the software immediately. This is the default.
- **+*minutes***—Number of minutes from now to reboot the software.
- ***yymmddhhmm***—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- ***hh:mm***—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

in *minutes*—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +*minutes*** option.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.

- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk)—(Optional) Boot medium for next boot.

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

- **external**—Reboot the external mass storage device.
- **internal**—Reboot the internal flash device.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc *number*—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace *number* with 0.

slice *slice*—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

- **1**—Power off partition 1.
- **2**—Power off partition 2.

- **alternate**—Reboot from the alternate partition.

Additional Information Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).

On a TX Matrix or TX Matrix Plus router, if you issue the **request system reboot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.



NOTE: Before issuing the **request system reboot** command on a TX Matrix Plus router with no options or the **all-chassis**, **all-lcc**, **lcc number**, or **sfc** options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the **request system reboot** command.



NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level maintenance

Related Documentation

- *clear system reboot*
- *request system halt*
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output

[request system reboot on page 313](#)
[request system reboot \(at 2300\) on page 313](#)
[request system reboot \(in 2 Hours\) on page 313](#)
[request system reboot \(Immediately\) on page 313](#)
[request system reboot \(at 1:20 AM\) on page 313](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes
```

```
shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

request system reboot

Syntax	<pre>request system reboot <all-members local member member-id> <at time> <in minutes> <media (external internal)> <message "text"> <slice (1 2 alternate)></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option partition changed to slice in Junos OS Release 10.0 for EX Series switches.</p>
Description	<p>Reboot the Junos OS.</p> <p>Reboot requests are recorded in the system log files, which you can view with the show log command. You can view the process names with the show system processes command.</p>
Options	<p>none—Reboots the software immediately.</p> <p>all-members local member member-id—(Optional) Specify which member of the Virtual Chassis to reboot:</p> <ul style="list-style-type: none"> • all-members—Reboots each switch that is a member of the Virtual Chassis. • local—Reboots the local switch, meaning the switch you are logged into, only. • member member-id—Reboots the specified member switch of the Virtual Chassis. <p>at time—(Optional) Time at which to reboot the software, specified in one of the following ways:</p> <ul style="list-style-type: none"> • +minutes—Number of minutes from now to reboot the software. • hh:mm—Absolute time on the current day at which to reboot the software, specified in 24-hour time. • now—Stop or reboot the software immediately. This is the default. • yymmddhhmm—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute. <p>in minutes—(Optional) Number of minutes from now to reboot the software. This option is an alias for the at +minutes option.</p> <p>media (external internal)—(Optional) Boot medium for the next boot. The external option reboots the switch using a software package stored on an external boot source, such as a USB flash drive. The internal option reboots the switch using a software package stored in an internal memory source.</p> <p>message "text"—(Optional) Message to display to all system users before rebooting the software.</p>

slice (1 | 2 | alternate)—(Optional) Reboot using the specified partition on the boot media.

This option has the following suboptions:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition, which is the partition that did not boot the switch at the last bootup.

Required Privilege Level maintenance

Related Documentation

- *clear system reboot*

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

request system reboot (Junos OS with Upgraded FreeBSD)

Syntax	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local> <media (oam junos network usb)> <member <i>member-id</i>> <message "<i>text</i>"> <other-routing-engine></pre>
Release Information	<p>Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.</p>
Description	Reboot the software.
Options	<p>none—Reboot the software immediately.</p> <p>all-members—(Optional) Reboot the software on all members of the Virtual Chassis configuration.</p> <p>at <i>time</i>—(Optional) Time at which to reboot the software, specified in one of the following ways:</p> <ul style="list-style-type: none"> now—Stop or reboot the software immediately. This is the default. +<i>minutes</i>—Number of minutes from now to reboot the software. <i>yymmddhhmm</i>—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute. Omitting a value will default to the current date for that value. <i>hh:mm</i>—Absolute time on the current day at which to stop the software, specified in 24-hour time. <p>both-routing-engines—(Optional) Reboot both Routing Engines at the same time.</p> <p>in <i>minutes</i>—(Optional) Number of minutes from now to reboot the software. This option is an alias for the at +<i>minutes</i> option.</p> <p>local—(Optional) Reboot the software on the local Virtual Chassis member.</p> <p>media (oam junos network usb)—(Optional) Reboot the boot media:</p> <ul style="list-style-type: none"> oam—Reboot from the oam volume. junos—Reboot from the junos volume. network—Reboot from the network. usb—Reboot from the USB device.

member *member-id*—(Optional) Reboot the software on the specified member of the Virtual Chassis configuration. Replace *member-id* with a value of 0 or 1.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

Additional Information Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).



NOTE: To reboot a router or switch that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level maintenance

Related Documentation

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [show system snapshot \(Junos OS with Upgraded FreeBSD\) on page 413](#)
- [clear system reboot](#)
- [request system halt](#)
- [Understanding Junos OS with Upgraded FreeBSD on page 19](#)

List of Sample Output

[request system reboot on page 317](#)
[request system reboot \(at 2300\) on page 317](#)
[request system reboot \(in 2 Hours\) on page 318](#)
[request system reboot \(Immediately\) on page 318](#)
[request system reboot \(at 1:20 AM\) on page 318](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message "Maintenance time!"
```

```
Reboot the system ? [yes,no] (no) yes
```

```
shutdown: [pid 186]
```

```
*** System shutdown message from root@berry.network.net ***
```

```
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
```

```
user@host> request system reboot in 120
```

```
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
```

```
request system reboot at 120
```

```
Reboot the system at 120? [yes,no] (no) yes
```

request system scripts add

Syntax	<code>request system scripts add <package-name></code> <code><no-copy></code> <code><unlink></code>
Release Information	Command introduced before Junos OS Release 9.0.
Description	CLI command to install AI-Script (jais) packages on Juniper Networks devices.
Options	no-copy —Don't save a copy of the jais package file. user@host> <code>request system scripts add no-copy <package-name></code>



NOTE: If you use the no-copy option during the jais installation, the jais package cannot be rolled back.

unlink—Remove the package after successful installation.

user@host> `request system scripts add unlink <package-name>`

Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system scripts delete on page 320 • request system scripts rollback on page 321 • <i>request system scripts event-scripts</i>

request system scripts delete

Syntax	<code>request system scripts delete <package-name></code>
Release Information	Command introduced before Junos OS Release 9.0.
Description	CLI command to delete AI-Script (jais) packages on Juniper Networks devices.
Options	No options are available.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system scripts add on page 319• request system scripts rollback on page 321• <i>request system scripts event-scripts</i>

request system scripts rollback

Syntax	<code>request system scripts rollback</code>
Release Information	Command introduced before Junos OS Release 9.0.
Description	Attempt to roll back to most recent installation of AI-Scripts (jais) package.
Options	No options are available.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system scripts add on page 319• request system scripts delete on page 320• <i>request system scripts event-scripts</i>

request system snapshot

List of Syntax	Syntax on page 322 Syntax (ACX Series Routers) on page 322 Syntax (EX Series Switches) on page 322 Syntax (MX Series Routers) on page 322 Syntax (TX Matrix Routers) on page 322 Syntax (TX Matrix Plus Routers) on page 322
Syntax	request system snapshot <partition>
Syntax (ACX Series Routers)	request system snapshot <media type> <partition>
Syntax (EX Series Switches)	request system snapshot <all-members local member <i>member-id</i> > <media type> <partition> <re0 re1 routing-engine <i>routing-engine-id</i> > <slice alternate>
Syntax (MX Series Routers)	request system snapshot <all-members> <config-partition> <local> <member <i>member-id</i> > <media <i>usb-port-number</i> > <partition> <root-partition>
Syntax (TX Matrix Routers)	request system snapshot <all-chassis all-lcc lcc <i>number</i> scc> <config-partition> <partition> <root-partition>
Syntax (TX Matrix Plus Routers)	request system snapshot <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> > <config-partition> <partition> <root-partition>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 10.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.2 for ACX Series switches.</p> <p>Options <config-partition> and <root-partition> introduced in Junos OS Release 13.1 for M, MX, T, TX Series switches.</p> <p>Option media <i>usb-port-number</i> introduced in Junos OS Release 13.2 for MX104 routers.</p> <p>Options <config-partition>, <root-partition>, and <slice> deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.</p>



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).

- Description**
- On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.
 - On the switch, take a snapshot of the files currently used to run the switch—the complete contents of the root (/), **/altroot**, **/config**, **/var**, and **/var-tmp** directories, which include the running Junos OS, the active configuration, and log files.



CAUTION: After you run the **request system snapshot** command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Options The specific options available depend upon the router or switch:

none—Back up the currently running software as follows:

- On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to **/altroot**, and **/config** is backed up to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard drive.
- On the switch, take a snapshot of the files currently used to run the switch and copy them to the media that the switch did not boot from. If the switch is booted from internal media, the snapshot is copied to external (USB) media. If the switch is booted from external (USB) media, the snapshot is copied to internal media.
 - If the snapshot destination is external media but a USB flash drive is not connected, an error message is displayed.
 - If the automatic snapshot procedure is already in progress, the command returns the following error: **Snapshot already in progress. Cannot start manual snapshot**. For additional information about the automatic snapshot feature, see [“Understanding Resilient Dual-Root Partitions on Switches” on page 95](#).

all-chassis | all-lcc | lcc *number* —(TX Matrix and TX Matrix Plus router only) (Optional)

- all-chassis**—On a TX Matrix router, archive data and executable areas for all Routing Engines in the chassis. On a TX Matrix Plus router, archive data and executable areas for all Routing Engines in the chassis.

- **all-lcc**—On a TX Matrix router, archive data and executable areas for all T640 routers (or line-card chassis) connected to a TX Matrix router. On a TX Matrix Plus router, archive data and executable areas for all routers (or line-card chassis) connected to a TX Matrix Plus router.
- **lcc *number***—On a TX Matrix router, archive data and executable areas for a specific T640 router (or line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, archive data and executable areas for a specific router (line-card chassis) that is connected to a TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

all-members | local | member *member-id*—(EX Series switch Virtual Chassis and MX Series routers only) (Optional) Specify where to place the snapshot (archive data and executable areas) in a Virtual Chassis:

- **all-members**—Create a snapshot (archive data and executable areas) for all members of the Virtual Chassis.
- **local**—Create a snapshot (archive data and executable areas) on the member of the Virtual Chassis that you are currently logged into.
- **member *member-id***—Create a snapshot (archive data and executable areas) for the specified member of the Virtual Chassis.

config-partition—(M, MX, T, TX Series routers only) Create a snapshot of the configuration partition only and store it onto the default **/altconfig** on the hard disk device or an **/altconfig** on a USB device.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in [“Understanding Junos OS with Upgraded FreeBSD” on page 19](#).

media *type*—(ACX Series, M320, T640, MX960 routers, and EX Series switches only)(Optional) Specify the boot device the software is copied to:

- **compact-flash**—Copy software to the primary compact flash drive.
- **external**—(Switches only) Copy software to an external mass storage device, such as a USB flash drive. If a USB drive is not connected, the switch displays an error message.
- **internal**—Copy software to an internal flash drive.
- **removable-compact-flash**—Copy software to the removable compact flash drive.
- **usb**—(ACX Series, M320, T640, MX960 routers only) Copy software to the device connected to the USB port.
- **usb0**—(MX104 routers only) Copy software to the device connected to the USB0 port.
- **usb1**—(MX104 routers only) Copy software to the device connected to the USB1 port.

partition—(Optional) Repartition the flash drive before a snapshot occurs. If the partition table on the flash drive is corrupted, the **request system snapshot** command fails and reports errors. The partition option is only supported for restoring the software image from the hard drive to the flash drive.

(Routers only) You cannot issue the request system snapshot command when you enable flash disk mirroring. We recommend that you disable flash disk mirroring when you upgrade or downgrade the software. For more information, see the *Junos OS Administration Library for Routing Devices*.

(EX Series switches only) If the snapshot destination is the media that the switch did not boot from, you must use the **partition** option.

re0 | re1 | routing-engine routing-engine-id—(EX6200 and EX8200 switches only) Specify where to place the snapshot in a redundant Routing Engine configuration.

- **re0**—Create a snapshot on Routing Engine 0.
- **re1**—Create a snapshot on Routing Engine 1.
- **routing-engine routing-engine-id**—Create a snapshot on the specified Routing Engine.

root-partition—(M, MX, T, TX Series routers only) Create a snapshot of the root partition only and store it onto the default **/altroot** on the hard disk device or an **/altroot** on a USB device.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

slice alternate—(EX Series switches only) (Optional) Take a snapshot of the active root partition and copy it to the alternate slice on the boot media.

Option deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

scc—(TX Matrix router only) (Optional) Archive data and executable areas for a TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus router only) (Optional) Archive data and executable areas for a TX Matrix Plus router (or switch-fabric chassis). Replace *number* with 0.

Additional Information

- (Routers only) Before upgrading the software on the router, when you have a known stable system, issue the **request system snapshot** command to back up the software, including the configuration, to the **/altroot** and **/altconfig** file systems. After you have upgraded the software on the router and are satisfied that the new packages are successfully installed and running, issue the **request system snapshot** command again to back up the new software to the **/altroot** and **/altconfig** file systems.
- (Routers only) You cannot issue the **request system snapshot** command when you enable flash disk mirroring. We recommend that you disable flash disk mirroring when you upgrade or downgrade the software. For more information, see the *Junos OS Administration Library for Routing Devices*.
- (TX Matrix and TX Matrix Plus router only) On a routing matrix, if you issue the **request system snapshot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are backed up. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are backed up.

Required Privilege Level maintenance

Related Documentation

- [request system snapshot \(Junos OS with Upgraded FreeBSD\) on page 329](#)
- [show system snapshot on page 410](#)
- [show system auto-snapshot on page 394](#)

List of Sample Output

[request system snapshot \(Routers\) on page 327](#)
[request system snapshot \(EX Series Switches\) on page 327](#)
[request system snapshot \(When the Partition Flag Is On\) on page 327](#)
[request system snapshot \(MX104 routers when media device is missing\) on page 327](#)
[request system snapshot \(When Mirroring Is Enabled\) on page 327](#)
[request system snapshot all-lcc \(Routing Matrix\) on page 327](#)

[request system snapshot all-members \(Virtual Chassis\) on page 328](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output[request system snapshot \(Routers\)](#)

```
user@host> request system snapshot
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
umount: /altconfig: not currently mounted
Copying /config to /altconfig.. (this may take a few minutes)
```

The following filesystems were archived: / /config

[request system snapshot \(EX Series Switches\)](#)

```
user@switch> request system snapshot partition
Clearing current label...
Partitioning external media (/dev/da1) ...
Partitions on snapshot:

    Partition Mountpoint Size Snapshot argument
    s1a      /altroot    179M none
    s2a      /           180M none
    s3d      /var/tmp     361M none
    s3e      /var        121M none
    s4d      /config      60M  none
Copying '/dev/da0s1a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2a' to '/dev/da1s2a' .. (this may take a few minutes)
Copying '/dev/da0s3d' to '/dev/da1s3d' .. (this may take a few minutes)
Copying '/dev/da0s3e' to '/dev/da1s3e' .. (this may take a few minutes)
Copying '/dev/da0s4d' to '/dev/da1s4d' .. (this may take a few minutes)
The following filesystems were archived: /altroot / /var/tmp /var /config
```

[request system snapshot \(When the Partition Flag Is On\)](#)

```
user@host> request system snapshot partition
Performing preliminary partition checks ...
Partitioning ad0 ...
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
```

The following filesystems were archived: / /config

[request system snapshot \(MX104 routers when media device is missing\)](#)

```
user@host > request system snapshot media usb0
error: usb0 media missing or invalid
```

[request system snapshot \(When Mirroring Is Enabled\)](#)

```
user@host> request system snapshot
Snapshot is not possible since mirror-flash-on-disk is configured.
```

[request system snapshot all-lcc \(Routing Matrix\)](#)

```
user@host> request system snapshot all-lcc
lcc0-re0:
```

```
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

lcc2-re0:

```
-----
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system snapshot all-members (Virtual Chassis)

```
user@switch> request system snapshot all-members media internal
```

fpc0:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

fpc1:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

fpc2:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

fpc3:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```


fpc4:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```

fpc5:

```
-----
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
```


request system snapshot (Junos OS with Upgraded FreeBSD)

Syntax	request system snapshot <delete <i>snapshot-name</i> > <load <i>snapshot-name</i> > <media <i>type</i> > <recovery>
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches. Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.
Description	On the router or switch, back up the currently running and active file system partitions to standby partitions that are not running. Non-recovery snapshots are named snap.date.time and stored in the /packages/sets directory.
<div>  <p>CAUTION: After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.</p> </div>	
Options	<p>none—On the router or switch, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, this creates a non-recovery snapshot named snap.<date>.<time> which is stored in /packages/sets.</p> <p>delete <i>snapshot-name</i>—(Optional) Delete a specific non-recovery snapshot from /packages/sets. Wildcards are supported, so request system snapshot delete snap* deletes all snapshots.</p> <p>load <i>snapshot-name</i>—(Optional) Load a specific snapshot from /packages/sets.</p> <p>media <i>type</i>—(Optional) Specify the boot device the software is copied to:</p> <ul style="list-style-type: none"> usb—(MX960 routers only) Copy software to the device connected to the USB port. <p>recovery—Create a recovery snapshot and store it in the /oam volume.</p>
Additional Information	Before upgrading the software on the router or switch, when you have a known stable system, issue the request system snapshot command to back up the software, including the configuration, to the /packages/sets file systems. After you have upgraded the software on the router or switch and are satisfied that the new packages are successfully installed and running, issue the request system snapshot command again to back up the new software to the /packages/sets file systems.
Required Privilege Level	maintenance

Related Documentation	<ul style="list-style-type: none">• request system reboot (Junos OS with Upgraded FreeBSD) on page 316• show system snapshot (Junos OS with Upgraded FreeBSD) on page 413• Understanding Junos OS with Upgraded FreeBSD on page 19
List of Sample Output	request system snapshot recovery on page 330 request system snapshot delete on page 330 request system snapshot on page 330
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system snapshot recovery](#)

```
user@host> request system snapshot recovery
Creating image ...
Compressing image . . .
Image size is 777MB

Recovery snapshot created successfully
```

[request system snapshot delete](#)

```
user@host> request system snapshot delete snap.20150112.122106
NOTICE: Snapshot 'snap.20150112.122106' deleted successfully
```

[request system snapshot](#)

```
user@host> request system snapshot
NOTICE: Snapshot snap.20150119.122106 created successfully
```

request system snapshot (SRX Series)

Syntax request system snapshot
 <factory>
 <media (compact-flash | hard-disk | internal | usb)>
 <node (all | local | node-id | primary)>
 <partition>
 <slice (alternate) >

Release Information Command introduced in Junos OS Release 10.2.

Description Back up the currently running and active file system partitions on the device.

- Options**
- **media—** (Optional) Specifies the media to be included in the snapshot:
 - **compact-flash—** Copies the snapshot to the CompactFlash card.
 - **hard-disk—** Copies the snapshot to the hard disk.
 - **usb—** Copies the snapshot to the USB storage device.
 - **node—** (Optional) Specifies the archive data and executable areas of a specific node.
 - **node-id—** Specifies for node(0, 1).
 - **all—** Specifies for all nodes.
 - **local—** Specifies for local nodes.
 - **primary—** Specifies for primary nodes.
 - **partition -** (Default) Specifies that the target media should be repartitioned before the backup is saved to it.



NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

Example: request system snapshot media usb partition

Example: request system snapshot media usb partition factory

- **slice—** (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
- **alternate—** (Optional) Stores the snapshot on the other root partition in the system.



NOTE: The slice option cannot be used along with the other request system snapshot options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	request system snapshot media hard-disk on page 332 request system snapshot media usb (when usb device is missing on page 332 request system snapshot media compact-flash on page 332 request system snapshot partition on page 332
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

[request system snapshot media usb \(when usb device is missing](#)

```
user@host> request system snapshot media usb
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

[request system snapshot media compact-flash](#)

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

[request system snapshot partition](#)

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system software abort in-service-upgrade (ICU)

Syntax	request system software abort in-service-upgrade
Release Information	Command introduced in Junos OS Release 11.2.
Description	Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the request system in-service-upgrade command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>request system software in-service-upgrade (Maintenance)</i>
List of Sample Output	request system software abort in-service-upgrade on page 333
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

request system software add

- List of Syntax**
- Syntax on page 334
 - Syntax (EX Series Switches) on page 334
 - Syntax (TX Matrix Router) on page 334
 - Syntax (TX Matrix Plus Router) on page 335
 - Syntax (MX Series Router) on page 335
 - Syntax (QFX Series) on page 335
 - Syntax (OCX Series) on page 335

Syntax *Reviewer: Can you use this command on OCX? Or does ONIE method replace this entirely?*

```
request system software add package-name
<best-effort-load>
<delay-restart>
<device-alias alias-name>
<force>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<satellite slot-id>
<set [package-name package-name]>
<unlink>
<upgrade-group [all | upgrade-group-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
<satellite slot-id>
<validate>
<version version-string>
```

Syntax (EX Series Switches)

```
request system software add package-name
<best-effort-load>
<delay-restart>
<force>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [package-name package-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
<validate>
```

Syntax (TX Matrix Router)

```
request system software add package-name
<best-effort-load>
<delay-restart>
<force>
<lcc number | scc>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [package-name package-name]>
```

	<unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i> > <validate>
Syntax (TX Matrix Plus Router)	request system software add <i>package-name</i> <best-effort-load> <delay-restart> <force> <lcc <i>number</i> sfc <i>number</i> > <no-copy> <no-validate> <re0 re1> <reboot> <set [<i>package-name package-name</i>]> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i> > <validate>
Syntax (MX Series Router)	request system software add <i>package-name</i> <best-effort-load> <delay-restart> <device-alias <i>alias-name</i> > <force> <member <i>member-id</i> > <no-copy> <no-validate> <re0 re1> <reboot> <satellite <i>slot-id</i> > <set [<i>package-name package-name</i>]> <upgrade-group [all <i>upgrade-group-name</i>]> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i> > <validate> <version <i>version-string</i> >
Syntax (QFX Series)	request system software add <i>package-name</i> <best-effort-load> <component all> <delay-restart> <force> <force-host> <no-copy> <no-validate> <partition> <reboot> <unlink> <upgrade-with-config> <upgrade-with-config-format <i>format</i> > <validate>
Syntax (OCX Series)	<i>Reviewer: Is this command still supported? If so, is this the correct syntax for OCX?</i>

```
request system software add package-name
<best-effort-load>
<delay-restart>
<force>
<force-host>
<no-copy>
<no-validate>
<reboot>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format format>
<validate>
```

Release Information Command introduced before Junos OS Release 7.4.
best-effort-load and **unlink** options added in Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
set [package-name package-name] option added in Junos OS Release 11.1 for EX Series switches.
set [package-name package-name] option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.



NOTE: On EX Series switches, the **set [package-name package-name]** option allows you to install only two software packages on a mixed EX4200 and EX4500 Virtual Chassis, whereas, on M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways, the **set [package-name package-name]** option allows you to install multiple software packages and software add-on packages at the same time.

upgrade-with-config and **upgrade-with-config-format *format*** options added in Junos OS Release 12.3 for M Series routers, MX Series routers, T Series routers, EX Series Ethernet switches, and QFX Series devices.

Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

device-alias, **satellite**, **upgrade-group**, and **version** options introduced in Junos OS Release 14.2R3 for Junos Fusion.

Description



NOTE: We recommend that you always download the software image to **/var/tmp** only. On EX Series and QFX Series switches, you must use the **/var/tmp** directory. Other directories are not supported.

Install a software package or bundle on the router or switch.



WARNING: Any configuration changes performed after inputting the `request system software add` command will be lost when the system reboots with an upgraded version of Junos OS.



NOTE: When graceful Routing Engine switchover (GRES) is enabled on a device, you must perform a unified ISSU operation to update the software running on the device. With GRES enabled, if you attempt to perform a software upgrade by entering the `request system software add package-name` command, an error message is displayed stating that only in-service-software-upgrades are supported when GRES is configured. In such a case, you must either remove the GRES configuration before you attempt the upgrade or perform a unified ISSU.

Options *package-name*—Location from which the software package or bundle is to be installed.

For example:

- */var/tmp/package-name*—For a software package or bundle that is being installed from a local directory on the router or switch.
- *protocol://hostname/pathname/package-name*—For a software package or bundle that is to be downloaded and installed from a remote location. Replace *protocol* with one of the following:
 - **ftp**—File Transfer Protocol.
Use *ftp://hostname/pathname/package-name*. To specify authentication credentials, use *ftp://<username>:<password>@hostname/pathname/package-name*. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required, and you do not specify the password or **prompt**, an error message is displayed.
 - **http**—Hypertext Transfer Protocol.
Use *http://hostname/pathname/package-name*. To specify authentication credentials, use *http://<username>:<password>@hostname/pathname/package-name*. If a password is required and you omit it, you are prompted for it.
 - **scp**—Secure copy (available only for Canada and U.S. version).
Use *scp://hostname/pathname/package-name*. To specify authentication credentials, use *scp://<username>:<password>@hostname/pathname/package-name*.

**NOTE:**

- The *pathname* in the protocol is the relative path to the user's home directory on the remote system and not the root directory.
- Do not use the `scp` protocol in the `request system software add` command to download and install a software package or bundle from a remote location. The previous statement does not apply to the QFabric switch. The software upgrade is handled by the MGD process which does not support `scp`.
Use the `file copy` command to copy the software package or bundle from the remote location to the `/var/tmp` directory on the hard disk:
`file copy scp://source/package-name /var/tmp`
Then install the software package or bundle using the `request system software add` command:
`request system software add /var/tmp/package-name`

best-effort-load—(Optional) Activate a partial load and treat parsing errors as warnings instead of errors.

component all—(QFabric systems only) (Optional) Install software package on all of the QFabric components.

delay-restart—(Optional) Install a software package or bundle, but do not restart software processes.

device-alias *alias-name*—(Junos Fusion only) (Optional) Install the satellite software package onto the specified satellite device using the satellite device's alias name.

force—(Optional) Force the addition of the software package or bundle (ignore warnings).

force-host—(Optional) Force the addition of host software package or bundle (ignore warnings) on the QFX5100 device.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) In a routing matrix based on the TX Matrix router, install a software package or bundle on a T640 router that is connected to the TX Matrix router. In a routing matrix based on the TX Matrix Plus router, install a software package or bundle on a router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.

- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

member *member-id*—(MX Series routers only) (Optional) Install a software package on the specified Virtual Chassis member. Replace *member-id* with a value of 0 or 1.

partition—(QFX3500 switches only) (Optional) Format and repartition the media before installation.

satellite *slot-id*—(Junos Fusion only) (Optional) Install the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

scc—(TX Matrix routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix Plus router. Replace *number* with 0.

no-copy—(Optional) Install a software package or bundle, but do not save copies of the package or bundle files.

no-validate—(Optional) When loading a software package or bundle with a different release, suppress the default behavior of the **validate** option.

re0 | re1—(Optional) On routers or switches that support dual or redundant Routing Engines, load a software package or bundle on the Routing Engine in slot 0 (re0) or the Routing Engine in slot 1 (re1).

reboot—(Optional) After adding the software package or bundle, reboot the system. On a QFabric switch, the software installation is not complete until you reboot the component for which you have installed the software.

set [*package-name package-name*]—(Mixed EX4200 and EX4500 Virtual Chassis only) (Optional) Install two software packages—a package for an EX4200 switch and the same release of the package for an EX4500 switch—to upgrade all member switches in a mixed EX4200 and EX4500 Virtual Chassis.

set [*package-name package-name*]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages and software add-on packages at the same time.

unlink—(Optional) On M Series, T Series, and MX Series routers, use the unlink option to remove the software package from this directory after a successful upgrade is completed.

upgrade-group [all |*upgrade-group-name*]—(Junos Fusion only) (Required to configure a Junos Fusion using autoconversion or manual conversion) Associate a satellite software image with a satellite software upgrade group. The satellite software package is associated with the specified satellite software upgrade group using the

upgrade-group-name, or for all satellite software upgrade groups in a Junos Fusion when the *all* keyword is specified.

A satellite software upgrade group is a group of satellite devices in a Junos Fusion that are designated to upgrade to the same satellite software version using the same satellite software package. See *Understanding Software in a Junos Fusion* and *Managing Satellite Software Upgrade Groups in a Junos Fusion*.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format *format*—(Optional) Specify the configuration file format, **text** or **xml**. The default format is **text**.



NOTE: The **upgrade-with-config** and **upgrade-with-config-format** options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the **.failed** suffix.

validate—(Optional) Validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle. This is the default behavior when the software package or bundle being added is a different release.



NOTE: The **validate** option only works on systems that do not have graceful-switchover (GRES) enabled. To use the **validate** option on a system with GRES, either disable GRES for the duration of the installation, or install using the command **request system software in-service-upgrade**, which requires nonstop active routing (NSR) to be enabled when using GRES.

version *version-string*—(Junos Fusion only) (Optional) Associate a satellite software package with a satellite software upgrade group by selecting the satellite software package's version. This option can only be used if the specified version of the satellite software has previously been installed on the aggregation device.

Additional Information Before upgrading the software on the router or switch, when you have a known stable system, issue the **request system snapshot** command to back up the software, including the configuration, to the **/altroot** and **/altconfig** file systems. After you have upgraded the software on the router or switch and are satisfied that the new package or bundle is

successfully installed and running, issue the **request system snapshot** command again to back up the new software to the **/altroot** and **/altconfig** file systems.



NOTE: The **request system snapshot** command is currently not supported on the QFabric system. Also, you cannot add or install multiple packages on a QFabric system.

After you run the **request system snapshot** command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

If you are upgrading more than one package at the same time, delete the operating system package, **jkernl**, last. Add the operating system package, **jkernl**, first and the routing software package, **jroute**, last. If you are upgrading all packages at once, delete and add them in the following order:

```
user@host> request system software add /var/tmp/jbase
user@host> request system software add /var/tmp/jkernl
user@host> request system software add /var/tmp/jpfe
user@host> request system software add /var/tmp/jdocs
user@host> request system software add /var/tmp/jroute
user@host> request system software add /var/tmp/jcrypto
```

By default, when you issue the **request system software add package-name** command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix backup Routing Engine, all the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, when you issue the **request system software add package-name** command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.

Required Privilege Level maintenance

Related Documentation

- [request system software delete on page 347](#)
- [request system software rollback on page 351](#)
- [request system storage cleanup on page 364](#)
- [Upgrading Software](#)
- [Upgrading Software on a QFabric System](#)
- [Managing Satellite Software Upgrade Groups in a Junos Fusion](#)
- [request system software add \(Maintenance\) on page 344](#)

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output	request system software add validate on page 342 request system software add (Mixed EX4200 and EX4500 Virtual Chassis) on page 343 request system software add component all (QFabric Systems) on page 343 request system software add upgrade-group (Junos Fusion) on page 343
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software add validate

```

user@host> request system software add validate /var/tmp/jinstall-7.2R1.7-domestic-signed.tgz
Checking compatibility with configuration
Initializing...
Using jbase-7.1R2.2
Using /var/tmp/jinstall-7.2R1.7-domestic-signed.tgz
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Using /var/validate/tmp/jinstall-signed/jinstall-7.2R1.7-domestic.tgz
Using /var/validate/tmp/jinstall/jbundle-7.2R1.7-domestic.tgz
Checking jbundle requirements on /
Using /var/validate/tmp/jbundle/jbase-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jkernel-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jcrypto-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jpfe-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jdocs-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jroute-7.2R1.7.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Validating against /config/rescue.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-7.2R1.7-domestic-signed.tgz' ...
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Adding jinstall...

WARNING: This package will load JUNOS 7.2R1.7 software.
WARNING: It will save JUNOS configuration files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. It will attempt to preserve dumps
WARNING: and log files, but this can not be guaranteed. This is the
WARNING: pre-installation stage and all the software is loaded when
WARNING: you reboot the system.

Saving the config files ...
Installing the bootstrap installer ...

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING: 'request system reboot' command when software installation is
WARNING: complete. To abort the installation, do not reboot your system,
WARNING: instead use the 'request system software delete jinstall'
WARNING: command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-7.2R1.7-domestic-signed.tgz ...
Saving state for rollback ...

```

Sample Output

request system software add (Mixed EX4200 and EX4500 Virtual Chassis)

```
user@switch> request system software add set
[/var/tmp/jinstall-ex-4200-11.1R1.1-domestic-signed.tgz
/var/tmp/jinstall-ex-4500-11.1R1.1-domestic-signed.tgz]
...
```

request system software add component all (QFabric Systems)

```
user@switch> request system software add /pbdata/packages/jinstall-qfabric-12.2X50-D1.3.rpm
component all
...
```

request system software add upgrade-group (Junos Fusion)

```
user@aggregation-device> request system software add /var/tmp/satellite-1.0R1.1-signed.tgz
upgrade-group group1
```

request system software add (Maintenance)

Syntax	<code>request system software add <i>package-name</i></code>
Release Information	Partition option introduced in the command in Junos OS Release 10.1.
Description	Install the new software package on the device. For example: request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.
Options	<ul style="list-style-type: none">• <code>delay-restart</code> — Installs the software package but does not restart the software process• <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors• <code>no-copy</code> — Installs the software package but does not saves the copies of package files• <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts• <code>partition</code> — Formats and re-partitions the media before installation• <code>reboot</code> — Reboots the device after installation is completed• <code>unlink</code> — Removes the software package after successful installation• <code>validate</code> — Checks the compatibility with current configuration before installation starts
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system reboot on page 1334

request system software configuration-backup

Syntax	request system software configuration-backup (<i>path</i>)
Release Information	Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Save the currently active configuration and any installation-specific parameters such as a configuration that you have entered outside of the CLI, Director group IP addresses, and the default partition IP address.
Options	path —(QFabric System) Provide the path to the location of the backup configuration files. You can save the backup configuration files to either a URL, local directory, remote server, or removable drive.
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none"> • request system software configuration-restore on page 346 • <i>Performing a QFabric System Recovery Installation on the Director Group</i>
List of Sample Output	request system software configuration-backup on page 345
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software configuration-backup

```

user@switch request system software configuration-backup ftp://ftp.test.net/test
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                               Dload  Upload  Total  Spent  Left
Speed
100      4035    0    0    100 4035    0    138k  --:--:-- --:--:-- --:--:--
0

```

request system software configuration-restore

Syntax	request system software configuration-restore (<i>path</i>)
Release Information	Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Restore a previously saved configuration and any installation-specific parameters, such as a configuration that you have entered outside of the CLI, Director group IP addresses, and the default partition IP address.
Options	path —(QFabric System) Provide the path to the location of the backup configuration files. The path can be to a local file, a file on an external flash drive, or an SCP or FTP destination.
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none"> • request system software configuration-backup on page 345 • <i>Performing a QFabric System Recovery Installation on the Director Group</i>
List of Sample Output	request system software configuration-restore on page 346
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output


request system software configuration-restore

```

user@switch request system software configuration-restore ftp://ftp.test.net/test
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload  Total    Spent    Left    Speed
100 4035 100 4035    0     0  153k      0  --:--:-- --:--:-- --:--:-- 3803k

```

request system software delete

List of Syntax	Syntax on page 347 Syntax (TX Matrix Router) on page 347 Syntax (TX Matrix Plus Router) on page 347
Syntax	<p><i>Reviewer: Can you use this command on OCX? Or does ONIE method replace this entirely?</i></p> <pre>request system software delete <i>software-package</i> <force> <reboot> <set [<i>package-name package-name</i>]> <upgrade-group [all <i>upgrade-group-name</i>]> <version <i>version-string</i>></pre>
Syntax (TX Matrix Router)	<pre>request system software delete <i>software-package</i> <force> <lcc <i>number</i> scc> <reboot> <set [<i>package-name package-name</i>]></pre>
Syntax (TX Matrix Plus Router)	<pre>request system software delete <i>software-package</i> <force> <lcc <i>number</i> sfc <i>number</i>> <reboot> <set [<i>package-name package-name</i>]></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Option set [<i>package-name package-name</i>] added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Services Gateways.</p> <p>Option reboot introduced in Junos OS Release 12.3.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Options upgrade-group, and version introduced in Junos OS Release 14.2R3 for Junos Fusion.</p>
Description	Remove a software package or bundle from the router or switch.
<div style="text-align: center;">  <p>CAUTION: Before removing a software package or bundle, make sure that you have already placed the new software package or bundle that you intend to load onto the router or switch.</p> </div>	
Options	<p><i>software-package</i>—Software package or bundle name. You can delete any or all of the following software bundles or packages:</p> <ul style="list-style-type: none"> jbase—(Optional) Junos base software suite jcrypto—(Optional, in domestic version only) Junos security software

- **jdocs**—(Optional) Junos online documentation file
- **jkernel**—(Optional) Junos kernel software suite
- **jpfe**—(Optional) Junos Packet Forwarding Engine support
- **jroute**—(Optional) Junos routing software suite
- **junos**—(Optional) Junos base software



NOTE: On EX Series switches, some of the package names are different than those listed. To see the list of packages that you can delete on an EX Series switch, enter the command **show system software**.

force—(Optional) Ignore warnings and force removal of the software.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) In a routing matrix, delete a software package or bundle on a T640 router indicated by **lcc number** that is connected to the TX Matrix router. In a routing matrix, delete a software package or bundle on a router indicated by **lcc number** that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

re0 | re1—(Optional) On routers or switches that support dual or redundant Routing Engines, delete a software package or bundle on the Routing Engine in slot 0 (**re0**) or the Routing Engine in slot 1 (**re1**).

reboot—As of Junos OS 12.3 and greater, automatically reboot upon completing the **request system software delete** command.

scc—(TX Matrix routers only) (Optional) Remove an extension or upgrade package from the TX Matrix router (or switch-card chassis).

set [package-name package-name]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

sfc number—(TX Matrix Plus routers only) (Optional) Remove an extension or upgrade package from the TX Matrix Plus router. Replace *number* with 0.

upgrade-group [**all** [*upgrade-group-name*]]—(Junos Fusion only) Delete the satellite software image association with the specified satellite software upgrade group.

A satellite software upgrade group is a group of satellite devices in the same Junos Fusion that are designated to upgrade to the same satellite software version using the same satellite software package.

version *version-string*—(Junos Fusion only) (Optional) Delete a satellite software package association with a satellite software upgrade group by selecting the satellite software package's version.

Additional Information Before upgrading the software on the router or switch, when you have a known stable system, issue the **request system snapshot** command to back up the software, including the configuration, to the /altroot and /altconfig file systems (on routers) or the /, /altroot, /config, /var, and /var/tmp file systems (on switches). After you have upgraded the software on the router or switch and are satisfied that the new packages are successfully installed and running, issue the **request system snapshot** command again to back up the new software to the /altroot and /altconfig file systems (on routers) or the /, /altroot, /config, /var, and /var/tmp file systems (on switches). After you run the **request system snapshot** command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Required Privilege Level maintenance

Related Documentation

- [request system software add on page 334](#)
- [request system software rollback on page 351](#)
- [request system software validate on page 357](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [request system software delete jdocs on page 349](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system software delete jdocs](#)

The following example displays the system software packages before and after the **jdocs** package is deleted through the **request system software delete** command:

```
user@host> show system software
Information for jbase:
```

```
Comment:
JUNOS Base OS Software Suite [7.2R1.7]
```

```
Information for jcrypto:
```

```
Comment:
JUNOS Crypto Software Suite [7.2R1.7]
```

Information for jdocs:

Comment:
JUNOS Online Documentation [7.2R1.7]

Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...

```
user@host> request system software delete jdocs
Removing package 'jdocs' ...
```

```
user@host> show system software
Information for jbase:
```

Comment:
JUNOS Base OS Software Suite [7.2R1.7]

Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [7.2R1.7]

Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...

request system software rollback

List of Syntax	Syntax on page 351 Syntax (EX Series Switches) on page 351 Syntax (TX Matrix Router) on page 351 Syntax (TX Matrix Plus Router) on page 351 Syntax (MX Series Router) on page 351
Syntax	request system software rollback
Syntax (EX Series Switches)	request system software rollback <all-members> <local> <member <i>member-id</i> > <reboot>
Syntax (TX Matrix Router)	request system software rollback <lcc <i>number</i> scc> <reboot>
Syntax (TX Matrix Plus Router)	request system software rollback <lcc <i>number</i> sfc <i>number</i> > <reboot>
Syntax (MX Series Router)	request system software rollback <all-members> <device-alias <i>alias-name</i> > <local> <member <i>member-id</i> > <reboot> <satellite <i>slot-id</i> > <upgrade-group [all <i>upgrade-group-name</i>]>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6. Command introduced in Junos OS Release 11.1 for the QFX Series. Command behavior changed in Junos OS Release 12.1. Option reboot introduced in Junos OS Release 12.3. Options device-alias , satellite , and upgrade-group introduced in Junos OS Release 14.2R3 for Junos Fusion. Option force deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

Description For all versions of Junos OS up to and including Junos OS 11.4, revert to the software that was loaded at the last successful **request system software add** command.

As of Junos OS 12.1 and greater, revert to the last known good state before the most recent **request system software (add | delete)** command. For example, using **rollback** in Junos OS 12.1 after using **request system software add** restores the system to a known good state prior to using the **add** command. Similarly, using **rollback** in Junos OS 12.1 after using **request system software delete** restores the system to a known good state prior to using the **delete** command.

A software rollback fails if any required package (or a **bundle** package containing the required package) cannot be found in `/var/sw/pkg`.

Additional Information

- On a Junos Fusion, the **request system software rollback** command can be used to roll back the version of satellite software associated with a satellite software upgrade group. Rolling back the version of satellite software associated with a satellite software upgrade group triggers a satellite software upgrade.
- On M Series and T Series routers, if **request system software add <jinstall> reboot** was used for the previous installation, then **request system software rollback** has no effect. In this case, use **jinstall** to reinstall the required package.
- On M Series and T Series routers, if **request system software add <sdk1>** was used for the previous installation, then **request system software rollback** removes the last installed SDK package (**sdk1** in this example).
- On SRX Series devices with dual root systems, when **request system software rollback** is run, the system switches to the alternate root. Each root can have a different version of Junos OS. Roll back takes each root back to the previously installed image.
- On QFX3500 and QFX3600 devices in a mixed Virtual Chassis, when the **request system software rollback** command is issued, the system does not rollback to the image stored in the alternate partition.
- On QFX5100 switches, the **reboot** option has been removed. To reboot the switch after a software rollback, issue the **request system reboot** command as a separate, secondary command.

Options **all-members**—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on all members of the Virtual Chassis configuration.

device-alias *alias-name*—(Junos Fusion only) (Optional) Rollback the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, attempt to roll back to the previous set of packages on a T640 router connected to the TX Matrix router. On a TX Matrix Plus router, attempt to roll back to the previous set of packages on a connected router connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the local Virtual Chassis member.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

none—For all versions of Junos OS up to and including Junos OS 11.4, revert to the set of software as of the last successful **request system software add**. As of Junos OS 12.1 and greater, revert to the last known good state before the most recent **request system software (add | delete)** command.

reboot—As of Junos OS 12.3 and greater, automatically reboot upon completing the **request system software rollback** command.

satellite *slot-id*—(Junos Fusion only) (Optional) Roll back the satellite software package onto the specified satellite device using the satellite devices FPC slot identifier.

scc—(TX Matrix routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix Plus router. Replace *number* with 0.

upgrade-group [all | *upgrade-group-name*]—(Junos Fusion only) Roll back the satellite software image associated with the specified satellite software upgrade group, or for all satellite software upgrade groups in the Junos Fusion when **all** is entered.

Required Privilege Level

maintenance

Related Documentation

- [request system software abort](#)
- [request system software add on page 334](#)
- [request system software delete on page 347](#)
- [request system software validate on page 357](#)

- *request system configuration rescue delete*
- *request system configuration rescue save*
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [request system software rollback on page 355](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software rollback

```

user@host> request system software rollback
Verified SHA1 checksum of ./jbase-7.2R1.7.tgz
Verified SHA1 checksum of ./jdocs-7.2R1.7.tgz
Verified SHA1 checksum of ./jroute-7.2R1.7.tgz
Installing package './jbase-7.2R1.7.tgz' ...
Available space: 35495 require: 7335
Installing package './jdocs-7.2R1.7.tgz' ...
Available space: 35339 require: 3497
Installing package './jroute-7.2R1.7.tgz' ...
Available space: 35238 require: 6976
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd: commit complete
Restarting mgd ...
Restarting aprobed ...
Restarting apsd ...
Restarting cosd ...
Restarting fsad ...
Restarting fud ...
Restarting gcdrd ...
Restarting ilmid ...
Restarting irsd ...
Restarting l2tpd ...
Restarting mib2d ...
Restarting nasd ...
Restarting pppoed ...
Restarting rdd ...
Restarting rmopd ...
Restarting rtspd ...
Restarting sampled ...
Restarting serviced ...
Restarting snmpd ...
Restarting spd ...
Restarting vrrpd ...

WARNING: cli has been replaced by an updated version:
CLI release 7.2R1.7 built by builder on 2005-04-22 02:03:44 UTC
Restart cli using the new version ? [yes,no] (yes) yes

Restarting cli ...
user@host

```

request system software rollback (SRX Series)

Syntax	<code>request system software rollback <node-id></code>
Release Information	Command introduced in Junos OS Release 10.1. Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.
Description	Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback .
Options	<i>node-id</i> —Identification number of the chassis cluster node. It can be 0 or 1.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system reboot on page 1334

request system software validate

List of Syntax	Syntax on page 357 Syntax (TX Matrix Router) on page 357 Syntax (TX Matrix Plus Router) on page 357 Syntax (MX Series Router) on page 357
Syntax	<p><i>Reviewer: Can you use this command on OCX? Or does ONIE method replace this entirely?</i></p> <pre>request system software validate <i>package-name</i> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (TX Matrix Router)	<pre>request system software validate <i>package-name</i> <lcc <i>number</i> scc> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (TX Matrix Plus Router)	<pre>request system software validate <i>package-name</i> <lcc <i>number</i> sfc <i>number</i>> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Syntax (MX Series Router)	<pre>request system software validate <i>package-name</i> <member <i>member-id</i>> <set [<i>package-name package-name</i>]> <upgrade-with-config> <upgrade-with-config-format <i>format</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>set [<i>package-name package-name</i>] option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.</p> <p>upgrade-with-config and upgrade-with-config-format <i>format</i> options added in Junos OS Release 12.3 for M Series routers, MX Series routers, and T Series routers.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Validate candidate software against the current configuration of the router.
Options	<p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, validate the software bundle or package on a specific T640 router (or line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, validate the software bundle or package for a specific router that is connected to the TX Matrix Plus router.</p>

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

member *member-id*—(MX Series routers only) (Optional) Validate the software bundle or package on the specified member of the Virtual Chassis configuration. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

package-name—Name of the software bundle or package to test.

scc—(TX Matrix routers only) (Optional) Validate the software bundle or package for the TX Matrix router (or switch-card chassis).

set [*package-name package-name*]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

sfc *number*—(TX Matrix Plus routers only) (Optional) Validate the software bundle or package for the TX Matrix Plus router.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format *format*—(Optional) Specify the configuration file format, **text** or **xml**. The default format is **text**.



NOTE: The **upgrade-with-config** and **upgrade-with-config-format** options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the **.failed** suffix.

Additional Information By default, when you issue the **request system software validate** command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are validated. If you issue the same command on the TX Matrix backup Routing Engine, all

the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, if you issue the **request system software validate** command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are validated. If you issue the same command on a TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.

Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>request system software abort</i> • request system software add on page 334 • request system software delete on page 347 • request system software rollback on page 351 • Routing Matrix with a TX Matrix Plus Router Solutions Page
List of Sample Output	request system software validate (Successful Case) on page 359 request system software validate (Failure Case) on page 359
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software validate (Successful Case)

```

user@host> request system software validate /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Checking compatibility with configuration
Initializing...
Using /packages/jbase-5.3I20020122_1901_sjg
Using /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jbase-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jkernel-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jcrypto-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jpfe-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jdocs-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jroute-5.3I20020124_0520_sjg.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete

WARNING: cli has been replaced by an updated version:
CLI release 5.3I0 built by sjg on 2002-01-24 05:23:53 UTC
Restart cli using the new version ? [yes,no] (yes)

```

request system software validate (Failure Case)

```

user@host> request system software validate 6.3/
Pushing bundle to lcc0-re0
error: Failed to transfer package to lcc0-re0

user@host> request system software validate test

```

```
Pushing bundle to lcc0-re0
Pushing bundle to lcc2-re0

lcc0-re0:
gzip: stdin: not in gzip format
tar: child returned status 1
ERROR: Not a valid package: /var/tmp/test
```


request system software validate on (Junos OS with Upgraded FreeBSD)

Syntax (MX240, MX480, MX960, MX2010, MX2020 Routers only)	request system software validate on <host <i>host-name</i> [username <i>user-name</i>]> <routing-engine (re0 re1)>
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, MX2020 routers only.
Description	<p>Direct validation of a running configuration is not possible on a device running Junos OS with upgraded FreeBSD. Nevertheless, validation is an important step in the installation of an upgraded operating system. This command allows validation on a device that is not running Junos OS with upgraded FreeBSD.</p> <p>This command validates the current configuration on a Routing Engine that is not running Junos OS with upgraded FreeBSD or a remote host.</p>
Options	<p>The specific options available are:</p> <p>host <i>host-name</i> [username <i>user-name</i>]—Validate the current configuration on a remote host. The host-name is resolved through DNS. Optionally, you can supply a user-name to employ on the remote host. If you omit the user-name option, the currently logged-in user-name is sent to the remote host.</p> <p>routing-engine (re0 re1)—Validate the current configuration on another Routing Engine on the same device. The other Routing Engine cannot be running Junos OS with upgraded FreeBSD or the validation does not succeed.</p>
Additional Information	If the authenticity of the remote host cannot be established, you are prompted to continue the validation or not. If you choose not to continue, the validation process does not take place.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system reboot (Junos OS with Upgraded FreeBSD) on page 316 • show system snapshot (Junos OS with Upgraded FreeBSD) on page 413 • Understanding Junos OS with Upgraded FreeBSD on page 19
List of Sample Output	request system software validate on host on page 362 request system software validate on routing-engine on page 362
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software validate on host

```

user@host> request system software validate on host remote-validator
The authenticity of host 'remote-validator (192.168.164.174)' can't be established.
ECDSA key fingerprint is 73:d0:78:ce:8d:09:aa:92:4c:ce:45:52:1d:76:86:b5.
Are you sure you want to continue connecting (yes/no)? yes
Password: *****

Sending /var/tmp/config.tgz to remote-validator...
Validating /var/tmp/config.tgz on remote-validator...
Checking compatibility with configuration
Initializing...
Using jbase-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jruntime-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jkernel-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jroute-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jcrypto-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jweb-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using /var/tmp/config.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: warning: schema: init: 'logical-systems-vlans' contains-node 'juniper-config
  vlans': not found
mgd: commit complete
Validation succeeded

```

request system software validate on routing-engine

```

user@host> request system software validate on routing-engine re1

Sending /var/tmp/config.tgz to re1...
Validating /var/tmp/config.tgz on re1...
Checking compatibility with configuration
Initializing...
Using jbase-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jruntime-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jkernel-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jroute-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jcrypto-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using jweb-15.1-20150416.2
Verified manifest signed by PackageDevelopmentEc_2015
Using /var/tmp/config.tgz
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
mgd: warning: schema: init: 'logical-systems-vlans' contains-node 'juniper-config
  vlans': not found

```

```
mgd: commit complete  
Validation succeeded
```

request system storage cleanup

List of Syntax	Syntax on page 364 Syntax (EX Series Switches) on page 364 Syntax (MX Series Router) on page 364 Syntax (QFX Series) on page 364 Syntax (SRX Series) on page 364
Syntax	request system storage cleanup <dry-run>
Syntax (EX Series Switches)	request system storage cleanup <all-members> <dry-run> <local> <member <i>member-id</i> > <satellite [slot-id <i>slot-id</i> device-alias <i>alias-name</i>]>
Syntax (MX Series Router)	request system storage cleanup <all-members> <dry-run> <local> <member <i>member-id</i> > <satellite [slot-id <i>slot-id</i> device-alias <i>alias-name</i>]>
Syntax (QFX Series)	request system storage cleanup <component (<i>serial number</i> <i>UUID</i> all)> <director-group <i>name</i> > <dry-run> <infrastructure <i>name</i> > <interconnect-device <i>name</i> > <name-tag <i>name-tag</i> > <node-group <i>name</i> > <prune> <qfabric (component <i>name</i>) dry-run name-tag repository> <repository (core log)>
Syntax (SRX Series)	request system storage cleanup <dry-run>
Release Information	Command introduced in Junos OS Release 7.4. dry-run option introduced in Junos OS Release 7.6. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 9.2 for SRX Series. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series. satellite option introduced in Junos OS Release 14.2R3.
Description	Free storage space on the router or switch by rotating log files and proposing a list of files for deletion. User input is required for file deletion. On a QFabric system, you can delete debug files located on individual devices or on the entire QFabric system.

Options **all-members**—(EX4200 switches and MX Series routers only) (Optional) Delete files on the Virtual Chassis master Routing Engine only.



NOTE: To delete files on the other members of the Virtual Chassis configuration, log in to each backup Routing Engine and delete the files using the **request system storage cleanup local** command.

component (*UUID | serial number | all*)—(QFabric systems only) (Optional) Delete files located on individual QFabric system devices or on the entire QFabric system.

director-group *name*—(QFabric systems only) (Optional) Delete files on the Director group.

dry-run—(Optional) List files proposed for deletion (without deleting them).

infrastructure *name*—(QFabric systems only) (Optional) Delete files on the fabric control Routing Engine and fabric manager Routing Engine.

interconnect-device *name*—(QFabric systems only) (Optional) Delete files on the Interconnect device.

local—(EX4200 switches and MX Series routers only) (Optional) Delete files on the local Virtual Chassis member.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Delete files on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

name-tag *name-tag*—(QFabric systems only) (Optional) Delete debug files that match a specific regular expression.

node-group *name*—(QFabric systems only) (Optional) Delete files on the Node group.

prune—(QFabric systems only) (Optional) Delete debug files located in either the core or log debug repositories of a QFabric system device.

qfabric component *name*—(QFabric systems only) (Optional) Delete debug files located in the debug repositories of a QFabric system device.

repository (*core | log*)—(QFabric systems only) (Optional) Specify the repository on the QFabric system device for which you want to delete debug files.

satellite [*slot-id slot-id | device-alias alias-name*]—(Junos Fusion only) (Optional) Specify the satellite device in the Junos Fusion by FPC ID or device alias name for which you want to delete debug files.

Additional Information If logging is configured and being used, the **dry-run** option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait.” If no logging is currently under way, the output displays only a list of files to delete.

Required Privilege Level maintenance

List of Sample Output

[request system storage cleanup dry-run on page 367](#)
[request system storage cleanup on page 367](#)
[request system storage cleanup director-group \(QFabric Systems\) on page 367](#)
[request system storage cleanup infrastructure device-name \(QFabric Systems\) on page 369](#)
[request system storage cleanup interconnect-device device-name \(QFabric Systems\) on page 370](#)
[request system storage cleanup node-group group-name \(QFabric Systems\) on page 371](#)
[request system storage cleanup qfabric component device-name \(QFabric Systems\) on page 372](#)
[request system storage cleanup qfabric component device-name repository core \(QFabric Systems\) on page 372](#)
[request system storage cleanup qfabric component all \(QFabric Systems\) on page 373](#)

Output Fields [Table 45](#) describes the output fields for the **request system storage cleanup** command. Output fields are listed in the approximate order in which they appear.

Table 45: request system storage cleanup Output Fields

Field Name	Field Description
List of files to delete:	Shows list of files available for deletion.
Size	Size of the core-dump file.
Date	Last core-dump file modification date and time.
Name	Name of the core-dump file.
Directory to delete:	Shows list of directories available for deletion.
Repository scope:	Repository where core-dump files and log files are stored. The core-dump files are located in the core repository, and the log files are located in the log repository. The default Repository scope is shared since both the core and log repositories are shared by all of the QFabric system devices.
Repository head:	Name of the top-level repository location.
Repository name:	Name of the repository: core or log .
Creating list of debug artifacts to be removed under:	Shows location of files available for deletion.
List of debug artifacts to be removed under:	Shows list of files available for deletion.

Sample Output

request system storage cleanup dry-run

```
user@host> request system storage cleanup dry-run
Currently rotating log files, please wait.
This operation can take up to a minute.
```

List of files to delete:

Size	Date	Name
11.4K	Mar 8 15:00	/var/log/messages.1.gz
7245B	Feb 5 15:00	/var/log/messages.3.gz
11.8K	Feb 22 13:00	/var/log/messages.2.gz
3926B	Mar 16 13:57	/var/log/messages.0.gz
3962B	Feb 22 12:47	/var/log/sampled.1.gz
4146B	Mar 8 12:20	/var/log/sampled.0.gz
4708B	Dec 21 11:39	/var/log/sampled.2.gz
7068B	Jan 16 18:00	/var/log/messages.4.gz
13.7K	Dec 27 22:00	/var/log/messages.5.gz
890B	Feb 22 17:22	/var/tmp/sampled.pkts
65.8M	Oct 26 09:10	/var/sw/pkg/jinstall-7.4R1.7-export-signed.tgz
63.1M	Oct 26 09:13	/var/sw/pkg/jbundle-7.4R1.7.tgz

request system storage cleanup

```
user@host> request system storage cleanup
Currently rotating log files, please wait.
This operation can take up to a minute.
```

List of files to delete:

Size	Date	Name
11.4K	Mar 8 15:00	/var/log/messages.1.gz
7245B	Feb 5 15:00	/var/log/messages.3.gz
11.8K	Feb 22 13:00	/var/log/messages.2.gz
3926B	Mar 16 13:57	/var/log/messages.0.gz
11.6K	Mar 8 15:00	/var/log/messages.5.gz
7254B	Feb 5 15:00	/var/log/messages.6.gz
12.9K	Feb 22 13:00	/var/log/messages.8.gz
3726B	Mar 16 13:57	/var/log/messages.7.gz
3962B	Feb 22 12:47	/var/log/sampled.1.gz
4146B	Mar 8 12:20	/var/log/sampled.0.gz
4708B	Dec 21 11:39	/var/log/sampled.2.gz
7068B	Jan 16 18:00	/var/log/messages.4.gz
13.7K	Dec 27 22:00	/var/log/messages.5.gz
890B	Feb 22 17:22	/var/tmp/sampled.pkts
65.8M	Oct 26 09:10	/var/sw/pkg/jinstall-7.4R1.7-export-signed.tgz
63.1M	Oct 26 09:13	/var/sw/pkg/jbundle-7.4R1.7.tgz

Delete these files ? [yes,no] (yes)

request system storage cleanup director-group (QFabric Systems)

```
user@switch> request system storage cleanup director-group
List of files to delete:
```

Size	Date	Name
4.0K	2011-11-07 05:16:29	/tmp/2064.sfcauth
4.0K	2011-11-07 05:07:34	/tmp/30804.sfcauth
4.0K	2011-11-07 04:13:41	/tmp/26792.sfcauth

```

4.0K 2011-11-07 04:13:39 /tmp/26432.sfcauth
0 2011-11-07 07:45:40 /tmp/cluster_cleanup.log
1.3M 2011-11-07 07:39:11 /tmp/cn_monitor.20111107-052401.log
4.0K 2011-11-07 07:36:29 /tmp/clustat.28019.log
4.0K 2011-11-07 07:36:29 /tmp/clustat_x.28019.log
9.6M 2011-11-07 05:30:24 /tmp/sfc.2.log
4.0K 2011-11-07 05:28:11 /tmp/mgd-init.1320672491.log
248K 2011-11-07 05:19:24 /tmp/cn_monitor.20111107-045111.log
4.0K 2011-11-07 05:17:18 /tmp/clustat.3401.log
4.0K 2011-11-07 05:17:18 /tmp/clustat_x.3401.log
8.0K 2011-11-07 04:58:25 /tmp/mgd-init.1320670633.log
0 2011-11-07 04:54:01 /tmp/mysql_db_install_5.1.37.log
4.0K 2011-11-07 04:52:08 /tmp/cn_send.log
0 2011-11-07 04:52:00 /tmp/init_eth0.log
4.0K 2011-11-07 04:49:35 /tmp/install_interfaces.sh.log
4.0K 2011-11-07 04:48:15 /tmp/bootstrap.sh.log
160K 2011-11-07 04:47:43 /tmp/bootstrap_cleanup.log
38M 2011-11-07 04:42:42 /tmp/cn_monitor.20111104-110308.log
4.0K 2011-11-07 04:38:47 /tmp/clustat.30913.log
4.0K 2011-11-07 04:38:47 /tmp/clustat_x.30913.log
4.0K 2011-11-07 04:38:03 /tmp/dcf_upgrade.sh.remove.log
4.0K 2011-11-07 04:38:03 /tmp/peer_update.log
4.0K 2011-11-07 04:38:02 /tmp/dcf_upgrade.log
4.0K 2011-11-07 04:38:02 /tmp/perl_mark_upgrade.log
8.0K 2011-11-07 04:13:42 /tmp/install_dcf_rpm.log
4.0K 2011-11-07 04:13:06 /tmp/00_cleanup.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/ccif_patch_4410_4450.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/dcf-tools.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/initial.sh.1320667986.log
0 2011-11-07 04:13:06 /tmp/inventory.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/qf-db.sh.1320667986.log
4.0K 2011-11-07 04:13:06 /tmp/sfc.sh.1320667986.log
8.0K 2011-11-07 04:13:05 /tmp/jinstall-qfabric.log
8.0K 2011-11-04 11:10:24 /tmp/mgd-init.1320430192.log
4.0K 2011-11-04 11:07:03 /tmp/mysql_dcf_db_install.log
8.0K 2011-11-04 10:55:07 /tmp/ccif_patch_4410_4450.sh.1320429307.log
8.0K 2011-11-04 10:55:07 /tmp/initial.sh.1320429307.log
4.0K 2011-11-04 10:55:07 /tmp/inventory.sh.1320429307.log
8.0K 2011-11-04 10:55:07 /tmp/sfc.sh.1320429307.log
4.0K 2011-11-04 10:54:09 /tmp/ks-script-Ax0tz5.log
4.0K 2011-11-07 04:13:06 /tmp//sfc.sh.1320667986.log
8.0K 2011-11-04 10:55:07 /tmp//sfc.sh.1320429307.log

```

Directory to delete:

```

45M 2011-11-08 10:57:43 /tmp/sfc-captures

```

List of files to delete:

	Size	Date	Name
4.0K	2011-11-08	05:47:47	/tmp/5713.sfcauth
4.0K	2011-11-08	05:14:32	/tmp/14494.sfcauth
4.0K	2011-11-08	05:11:47	/tmp/9978.sfcauth
4.0K	2011-11-08	05:09:37	/tmp/6128.sfcauth
4.0K	2011-11-08	05:04:28	/tmp/29703.sfcauth
4.0K	2011-11-07	11:59:10	/tmp/7811.sfcauth
4.0K	2011-11-07	11:36:08	/tmp/32415.sfcauth
4.0K	2011-11-07	11:30:30	/tmp/22406.sfcauth
4.0K	2011-11-07	11:24:37	/tmp/12131.sfcauth
4.0K	2011-11-07	10:48:42	/tmp/12687.sfcauth
4.0K	2011-11-07	09:27:20	/tmp/31082.sfcauth
4.0K	2011-11-07	07:33:58	/tmp/14633.sfcauth


```

4.0K 2011-11-07 05:08:25 /tmp/15447.sfcauth
4.0K 2011-11-07 04:12:29 /tmp/26874.sfcauth
4.0K 2011-11-07 04:12:27 /tmp/26713.sfcauth
4.0K 2011-11-07 03:49:17 /tmp/17691.sfcauth
4.0K 2011-11-05 01:32:23 /tmp/5716.sfcauth
4.0K 2011-11-07 08:00:17 /tmp/sfcsnmpd.log
4.0K 2011-11-07 07:57:50 /tmp/cluster_cleanup.log
824K 2011-11-07 07:38:37 /tmp/cn_monitor.20111107-053643.log
4.0K 2011-11-07 07:36:30 /tmp/clustat.18399.log
4.0K 2011-11-07 07:36:30 /tmp/clustat_x.18399.log
4.0K 2011-11-07 07:35:47 /tmp/command_lock.log
4.0K 2011-11-07 05:39:54 /tmp/mgd-init.1320673194.log
92K 2011-11-07 05:19:25 /tmp/cn_monitor.20111107-050412.log
4.0K 2011-11-07 05:17:20 /tmp/clustat.30115.log
4.0K 2011-11-07 05:17:20 /tmp/clustat_x.30115.log
8.0K 2011-11-07 05:08:07 /tmp/mgd-init.1320671241.log
4.0K 2011-11-07 05:04:57 /tmp/cn_send.log
0 2011-11-07 05:04:52 /tmp/init_eth0.log
4.0K 2011-11-07 05:02:38 /tmp/install_interfaces.sh.log
4.0K 2011-11-07 05:01:19 /tmp/bootstrap.sh.log
160K 2011-11-07 05:00:47 /tmp/bootstrap_cleanup.log
28M 2011-11-07 04:42:27 /tmp/cn_monitor.20111104-112954.log
4.0K 2011-11-07 04:38:49 /tmp/clustat.6780.log
4.0K 2011-11-07 04:38:49 /tmp/clustat_x.6780.log
4.0K 2011-11-07 04:38:05 /tmp/issue_event.log
4.0K 2011-11-07 04:38:05 /tmp/peer_upgrade_reboot.log
12K 2011-11-07 04:38:05 /tmp/primary_update.log
4.0K 2011-11-07 04:38:04 /tmp/dcf_upgrade.sh.remove.log
4.0K 2011-11-07 04:38:04 /tmp/peer_rexec_upgrade.log
4.0K 2011-11-07 04:13:42 /tmp/peer_install_dcf_rpm.log
4.0K 2011-11-07 04:11:57 /tmp/dcf-tools.sh.1320667917.log
0 2011-11-07 04:11:57 /tmp/initial.sh.1320667917.log
0 2011-11-07 04:11:57 /tmp/inventory.sh.1320667917.log
4.0K 2011-11-07 04:11:57 /tmp/qf-db.sh.1320667917.log
4.0K 2011-11-07 04:11:57 /tmp/sfc.sh.1320667917.log
4.0K 2011-11-07 04:11:56 /tmp/00_cleanup.sh.1320667916.log
0 2011-11-07 04:11:56 /tmp/ccif_patch_4410_4450.sh.1320667916.log
8.0K 2011-11-07 04:11:56 /tmp/jinstall-qfabric.log
4.0K 2011-11-07 04:11:33 /tmp/dcf_upgrade.log
8.0K 2011-11-04 11:53:12 /tmp/mgd-init.1320432782.log
8.0K 2011-11-04 11:06:17 /tmp/ccif_patch_4410_4450.sh.1320429977.log
8.0K 2011-11-04 11:06:17 /tmp/initial.sh.1320429977.log
4.0K 2011-11-04 11:06:17 /tmp/inventory.sh.1320429977.log
8.0K 2011-11-04 11:06:17 /tmp/sfc.sh.1320429977.log
4.0K 2011-11-04 11:05:19 /tmp/ks-script_tnWeb.log
4.0K 2011-11-07 04:11:57 /tmp/sfc.sh.1320667917.log
8.0K 2011-11-04 11:06:17 /tmp/sfc.sh.1320429977.log

```

Directory to delete:

```
49M 2011-11-08 10:45:20 /tmp/sfc-captures
```

request system storage cleanup infrastructure device-name (QFabric Systems)

```
user@switch> request system storage cleanup infrastructure FC-0
re0:
```

List of files to delete:

Size	Date	Name
139B	Nov 8 19:03	/var/log/default-log-messages.0.gz

```

5602B Nov  8 19:03 /var/log/messages.0.gz
28.4K Nov  8 10:15 /var/log/messages.1.gz
35.2K Nov  7 13:45 /var/log/messages.2.gz
207B Nov  7 16:02 /var/log/wtmp.0.gz
27B Nov  7 12:14 /var/log/wtmp.1.gz
184.4M Nov  7 12:16
/var/sw/pkg/jinstall-dc-re-11.3I20111104_1216_dc-builder-domestic-signed.tgz
124.0K Nov  7 15:59 /var/tmp/gres-tp/env.dat
0B Nov  7 12:57 /var/tmp/gres-tp/lock
155B Nov  7 16:02 /var/tmp/krt_gencfg_filter.txt
0B Nov  7 12:35 /var/tmp/last_ccif_update
1217B Nov  7 12:15 /var/tmp/loader.conf.preinstall
184.4M Nov  6 07:11 /var/tmp/mchassis-install.tgz
10.8M Nov  7 12:16
/var/tmp/preinstall/bootstrap-install-11.3I20111104_1216_dc-builder.tar
57.4K Nov  7 12:16 /var/tmp/preinstall/configs-11.3I20111104_1216_dc-builder.tgz

259B Nov  7 12:16 /var/tmp/preinstall/install.conf
734.3K Nov  4 13:46
/var/tmp/preinstall/jboot-dc-re-11.3I20111104_1216_dc-builder.tgz
177.8M Nov  7 12:16
/var/tmp/preinstall/jbundle-dc-re-11.3I20111104_1216_dc-builder-domestic.tgz
124B Nov  7 12:15 /var/tmp/preinstall/metatags
1217B Nov  7 12:16 /var/tmp/preinstall_boot_loader.conf
0B Nov  7 16:02 /var/tmp/rtsdb/if-rtsdb

```

request system storage cleanup interconnect-device device-name (QFabric Systems)

```

user@switch> request system storage cleanup interconnect IC-WS001
re1:

```

List of files to delete:

Size	Date	Name
11B	Nov 7 15:55	/var/jail/tmp/alarmd.ts
128B	Nov 8 19:06	/var/log/default-log-messages.0.gz
9965B	Nov 8 19:06	/var/log/messages.0.gz
15.8K	Nov 8 12:30	/var/log/messages.1.gz
15.8K	Nov 8 11:00	/var/log/messages.2.gz
15.7K	Nov 8 07:30	/var/log/messages.3.gz
15.8K	Nov 8 04:00	/var/log/messages.4.gz
15.7K	Nov 8 00:30	/var/log/messages.5.gz
18.7K	Nov 7 21:00	/var/log/messages.6.gz
17.6K	Nov 7 19:00	/var/log/messages.7.gz
58.3K	Nov 7 16:00	/var/log/messages.8.gz
20.3K	Nov 7 15:15	/var/log/messages.9.gz
90B	Nov 7 15:41	/var/log/wtmp.0.gz
57B	Nov 7 12:41	/var/log/wtmp.1.gz
124.0K	Nov 7 15:42	/var/tmp/gres-tp/env.dat
0B	Nov 7 12:40	/var/tmp/gres-tp/lock
0B	Nov 7 12:41	/var/tmp/if-rtsdb/env.lck
12.0K	Nov 7 15:41	/var/tmp/if-rtsdb/env.mem
132.0K	Nov 7 15:55	/var/tmp/if-rtsdb/shm_usr1.mem
2688.0K	Nov 7 15:41	/var/tmp/if-rtsdb/shm_usr2.mem
2048.0K	Nov 7 15:41	/var/tmp/if-rtsdb/trace.mem
730B	Nov 7 19:57	/var/tmp/juniper.conf+.gz
155B	Nov 7 15:53	/var/tmp/krt_gencfg_filter.txt
0B	Nov 7 15:41	/var/tmp/rtsdb/if-rtsdb

re0:

List of files to delete:

	Size	Date	Name
	11B	Nov 7 15:55	/var/jail/tmp/alarmd.ts
	121B	Nov 8 19:06	/var/log/default-log-messages.0.gz
	16.7K	Nov 8 19:06	/var/log/messages.0.gz
	22.2K	Nov 8 17:45	/var/log/messages.1.gz
	18.4K	Nov 8 17:00	/var/log/messages.2.gz
	21.6K	Nov 8 16:00	/var/log/messages.3.gz
	17.9K	Nov 8 14:30	/var/log/messages.4.gz
	19.4K	Nov 8 13:30	/var/log/messages.5.gz
	18.2K	Nov 8 12:30	/var/log/messages.6.gz
	20.4K	Nov 8 11:30	/var/log/messages.7.gz
	21.4K	Nov 8 10:15	/var/log/messages.8.gz
	21.0K	Nov 8 09:00	/var/log/messages.9.gz
	19.9K	Nov 8 08:13	/var/log/snmp-traps.0.gz
	203B	Nov 8 15:36	/var/log/wtmp.0.gz
	57B	Nov 7 12:41	/var/log/wtmp.1.gz
	124.0K	Nov 7 15:42	/var/tmp/gres-tp/env.dat
	0B	Nov 7 12:40	/var/tmp/gres-tp/lock
	0B	Nov 7 12:41	/var/tmp/if-rtssdb/env.lck
	12.0K	Nov 7 15:41	/var/tmp/if-rtssdb/env.mem
	132.0K	Nov 7 15:55	/var/tmp/if-rtssdb/shm_usr1.mem
	2688.0K	Nov 7 15:41	/var/tmp/if-rtssdb/shm_usr2.mem
	2048.0K	Nov 7 15:41	/var/tmp/if-rtssdb/trace.mem
	727B	Nov 7 15:54	/var/tmp/juniper.conf+.gz
	155B	Nov 7 15:55	/var/tmp/krt_gencfg_filter.txt
	0B	Nov 7 15:41	/var/tmp/rtssdb/if-rtssdb

request system storage cleanup node-group group-name (QFabric Systems)

```
user@switch> request system storage cleanup node-group NW-NG-0
BBAK0372:
```

List of files to delete:

	Size	Date	Name
	126B	Nov 8 19:07	/var/log/default-log-messages.0.gz
	179B	Nov 7 13:32	/var/log/install.0.gz
	22.9K	Nov 8 19:07	/var/log/messages.0.gz
	26.5K	Nov 8 17:30	/var/log/messages.1.gz
	20.5K	Nov 8 13:15	/var/log/messages.2.gz
	33.2K	Nov 7 17:45	/var/log/messages.3.gz
	35.5K	Nov 7 15:45	/var/log/messages.4.gz
	339B	Nov 8 17:10	/var/log/wtmp.0.gz
	58B	Nov 7 12:40	/var/log/wtmp.1.gz
	124.0K	Nov 8 17:08	/var/tmp/gres-tp/env.dat
	0B	Nov 7 12:39	/var/tmp/gres-tp/lock
	0B	Nov 7 12:59	/var/tmp/if-rtssdb/env.lck
	12.0K	Nov 8 17:09	/var/tmp/if-rtssdb/env.mem
	2688.0K	Nov 8 17:09	/var/tmp/if-rtssdb/shm_usr1.mem
	132.0K	Nov 8 17:09	/var/tmp/if-rtssdb/shm_usr2.mem
	2048.0K	Nov 8 17:09	/var/tmp/if-rtssdb/trace.mem
	1082B	Nov 8 17:09	/var/tmp/juniper.conf+.gz
	155B	Nov 7 17:39	/var/tmp/krt_gencfg_filter.txt
	0B	Nov 8 17:09	/var/tmp/rtssdb/if-rtssdb

EE3093:

List of files to delete:

Size	Date	Name
11B	Nov 8 17:33	/var/jail/tmp/alarmd.ts
119B	Nov 8 19:08	/var/log/default-log-messages.0.gz
180B	Nov 7 17:41	/var/log/install.0.gz
178B	Nov 7 13:32	/var/log/install.1.gz
2739B	Nov 8 19:08	/var/log/messages.0.gz
29.8K	Nov 8 18:45	/var/log/messages.1.gz
31.8K	Nov 8 17:15	/var/log/messages.2.gz
20.6K	Nov 8 16:00	/var/log/messages.3.gz
15.4K	Nov 8 10:15	/var/log/messages.4.gz
15.4K	Nov 8 02:15	/var/log/messages.5.gz
25.5K	Nov 7 20:45	/var/log/messages.6.gz
48.0K	Nov 7 17:45	/var/log/messages.7.gz
32.8K	Nov 7 13:45	/var/log/messages.8.gz
684B	Nov 8 17:02	/var/log/wtmp.0.gz
58B	Nov 7 12:40	/var/log/wtmp.1.gz
124.0K	Nov 7 17:34	/var/tmp/gres-tp/env.dat
0B	Nov 7 12:40	/var/tmp/gres-tp/lock
0B	Nov 7 12:59	/var/tmp/if-rtssdb/env.lck
12.0K	Nov 7 17:39	/var/tmp/if-rtssdb/env.mem
2688.0K	Nov 7 17:39	/var/tmp/if-rtssdb/shm_usr1.mem
132.0K	Nov 7 17:40	/var/tmp/if-rtssdb/shm_usr2.mem
2048.0K	Nov 7 17:39	/var/tmp/if-rtssdb/trace.mem
155B	Nov 7 17:40	/var/tmp/krt_gencfg_filter.txt
0B	Nov 7 17:39	/var/tmp/rtssdb/if-rtssdb

request system storage cleanup qfabric component device-name (QFabric Systems)

```

user@switch> request system storage cleanup qfabric component A0001/YA0197
Repository type: regular
Repository head: /pbstorage
Creating list of debug artifacts to be removed under:
/pbstorage/rumps/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rumps/A0001/YA0197/cosd.core.0.0.05162011123308.gz ... done
Removing /pbstorage/rumps/A0001/YA0197/cosd.core.1.0.05162011123614.gz ... done
Removing /pbstorage/rumps/A0001/YA0197/cosd.core.2.0.05162011123920.gz ... done
Removing /pbstorage/rumps/A0001/YA0197/livecore.05132011163930.gz ... done
Removing /pbstorage/rumps/A0001/YA0197/tetnetd.core.0.1057.05162011124500.gz ...
done
Removing /pbstorage/rumps/A0001/YA0197/vmcore.05132011120528.gz ... done
Removing /pbstorage/rumps/A0001/YA0197/vmcore.kz ... done
Creating list of debug artifacts to be removed under: /pbstorage/rlogs/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rlogs/A0001/YA0197/kdumpinfo.05132011120528 ... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.0.1039.05122011234415.tgz
... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.1.1039.05132011175544.tgz
... done
Removing /pbstorage/rlogs/A0001/YA0197/tetnetd.tarball.0.1057.05162011175453.tgz
... done

```

request system storage cleanup qfabric component device-name repository core (QFabric Systems)

```

user@switch> request system storage cleanup qfabric component EE3093 repository core
Repository scope: shared
Repository head: /pbdata/export

```

```
Repository name: core
Creating list of debug artifacts to be removed under: /pbdata/export/rdumps/EE3093
NOTE: core repository under /pbdata/export/rdumps/EE3093 empty
```

request system storage cleanup qfabric component all (QFabric Systems)

```
user@switch> request system storage cleanup qfabric component all
Repository scope: shared
Repository head: /pbdata/export
Creating list of debug artifacts to be removed under: /pbdata/export/rdumps
NOTE: core repository under /pbdata/export/rdumps/all empty
Creating list of debug artifacts to be removed under: /pbdata/export/rlogs
List of debug artifacts to clean up ... (press control C to abort)
/pbdata/export/rlogs/73747cd8-0710-11e1-b6a4-00e081c5297e/install-11072011125819.log
/pbdata/export/rlogs/77116f18-0710-11e1-a2a0-00e081c5297e/install-11072011125819.log
/pbdata/export/rlogs/BBAK0372/install-11072011121538.log
/pbdata/export/rlogs/BBAK0394/install-11072011121532.log
/pbdata/export/rlogs/EE3093/install-11072011121536.log
/pbdata/export/rlogs/WS001/YN5999/install-11072011121644.log
/pbdata/export/rlogs/WS001/YW3803/install-11072011122429.log
/pbdata/export/rlogs/cd78871a-0710-11e1-878e-00e081c5297e/install-11072011125932.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011125930.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011133211.log
/pbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011155302.log
/pbdata/export/rlogs/d31ab7a6-0710-11e1-ad1b-00e081c5297e/install-11072011125931.log
/pbdata/export/rlogs/d4d0f254-0710-11e1-90c3-00e081c5297e/install-11072011125932.log
```

request system storage cleanup (SRX Series)

Syntax	<code>request system storage cleanup <dry-run></code>
Release Information	Command introduced in Junos OS Release 9.2 for SRX Series.
Description	Free storage space on the device by rotating log files and proposing a list of files for deletion. User input is required for file deletion.
Options	dry-run —(Optional) List files proposed for deletion (without deleting them).
Additional Information	If logging is configured and being used, the dry-run option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait.” If no logging is currently under way, the output displays only a list of files to delete.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> Cleaning Up Files with the CLI on page 1135
List of Sample Output	request system storage cleanup dry-run on page 374 request system storage cleanup on page 376
Output Fields	Table 45 describes the output fields for the request system storage cleanup command. Output fields are listed in the approximate order in which they appear.

Table 46: request system storage cleanup Output Fields

Field Name	Field Description
List of files to delete:	Shows list of files available for deletion.
Size	Size of the core-dump file.
Date	Last core-dump file modification date and time.
Name	Name of the core-dump file.

Sample Output

request system storage cleanup dry-run

```

user@host> request system storage cleanup dry-run
List of files to delete:

      Size Date      Name
11B Jul 14 22:51 /var/jail/tmp/alarmd.ts
84.3K Jul 20 22:09 /var/log/chassisd.0.gz
83.0K Jul 20 04:35 /var/log/chassisd.1.gz
84.0K Jul 19 10:52 /var/log/chassisd.2.gz
90.4K Jul 18 17:16 /var/log/chassisd.3.gz

```

```

91.8K Jul 20 04:30 /var/log/hostlogs/auth.log.1.gz
93.1K Jul 17 05:45 /var/log/hostlogs/auth.log.2.gz
97.6K Jun 7 01:30 /var/log/hostlogs/auth.log.3.gz
92.0K Apr 25 15:15 /var/log/hostlogs/auth.log.4.gz
78.0K Jul 21 05:44 /var/log/hostlogs/daemon.log.1.gz
78.6K Jul 21 02:59 /var/log/hostlogs/daemon.log.2.gz
78.5K Jul 21 00:14 /var/log/hostlogs/daemon.log.3.gz
78.8K Jul 20 21:30 /var/log/hostlogs/daemon.log.4.gz
58.7K Jul 21 05:14 /var/log/hostlogs/debug.1.gz
58.5K Jul 21 00:59 /var/log/hostlogs/debug.2.gz
58.7K Jul 20 20:44 /var/log/hostlogs/debug.3.gz
58.7K Jul 20 16:29 /var/log/hostlogs/debug.4.gz
166.9K Jul 13 00:33 /var/log/hostlogs/kern.log.1.gz
166.5K Jun 1 02:32 /var/log/hostlogs/kern.log.2.gz
163.5K May 5 00:03 /var/log/hostlogs/kern.log.3.gz
152.3K Mar 2 23:23 /var/log/hostlogs/kern.log.4.gz
260.0K Apr 13 10:28 /var/log/hostlogs/lcmd.log.1.gz
257.3K Mar 7 00:38 /var/log/hostlogs/lcmd.log.2.gz
240.8K Feb 7 19:45 /var/log/hostlogs/lcmd.log.3.gz
241.1K Feb 7 14:00 /var/log/hostlogs/lcmd.log.4.gz
370.6K Jul 21 00:45 /var/log/hostlogs/syslog.1.gz
370.9K Jul 20 12:30 /var/log/hostlogs/syslog.2.gz
370.4K Jul 20 00:15 /var/log/hostlogs/syslog.3.gz
370.2K Jul 19 12:00 /var/log/hostlogs/syslog.4.gz
55.0K Jul 14 22:50 /var/log/hostlogs/vjunos0.log.1.gz
1467B Oct 28 2015 /var/log/install.0.gz
119.9K Jul 21 07:37 /var/log/messages.0.gz
147.4K May 27 01:30 /var/log/messages.1.gz
71.4K Apr 14 11:19 /var/log/messages.2.gz
90.7K Feb 28 14:15 /var/log/messages.3.gz
10.1K Jan 12 2016 /var/log/messages.4.gz
55.1K Jan 6 2016 /var/log/messages.5.gz
81.5K Dec 1 2015 /var/log/messages.6.gz
43.3K Oct 28 2015 /var/log/messages.7.gz
54.8K Oct 20 2015 /var/log/messages.8.gz
35.8K Oct 19 2015 /var/log/messages.9.gz
12.4K Jul 21 07:37 /var/log/security.0.gz
59.4K Jul 19 01:30 /var/log/security.1.gz
51.8K Apr 25 10:00 /var/log/security.2.gz
43.6K Apr 14 11:19 /var/log/security.3.gz
52.7K Apr 5 02:15 /var/log/security.4.gz
54.4K Mar 25 17:15 /var/log/security.5.gz
51.9K Mar 16 05:15 /var/log/security.6.gz
52.0K Mar 5 02:15 /var/log/security.7.gz
53.4K Feb 22 22:15 /var/log/security.8.gz
55.6K Feb 13 13:00 /var/log/security.9.gz
4063B Jul 14 22:51 /var/tmp/cleanup-pkgs.log
0B Jul 14 22:51 /var/tmp/eedebug_bin_file
50.9K Feb 8 20:33 /var/tmp/event_tags.php
34B Jul 14 22:51 /var/tmp/gksdchk.log
124.0K Apr 26 06:12 /var/tmp/gres-tp/env.dat
0B Oct 9 2015 /var/tmp/gres-tp/lock
4B Jul 14 22:52 /var/tmp/idp_license_info
46B Jul 14 22:51 /var/tmp/kmdchk.log
57B Jul 14 22:51 /var/tmp/krt_rpf_filter.txt
30B Jul 14 22:53 /var/tmp/policy_status
0B Jul 14 22:51 /var/tmp/rtsdb/if-rtsdb
349B Jul 14 22:51 /var/tmp/sd-upgrade/debug_log
0B Oct 9 2015 /var/tmp/spu_kmd_init
53B Feb 7 23:11 /var/tmp/vjunos-install.log
0B Jul 14 22:51 /var/tmp/vpn_tunnel_orig.id

```

request system storage cleanup

```
user@host> request system storage cleanup
```

```
List of files to delete:
```

	Size	Date	Name
	11B	Oct 28 23:40	/var/jail/tmp/alarmd.ts
	92.4K	Jan 11 17:12	/var/log/chassisd.0.gz
	92.4K	Jan 11 06:06	/var/log/chassisd.1.gz
	92.5K	Jan 10 19:00	/var/log/chassisd.2.gz
	92.5K	Jan 10 07:53	/var/log/chassisd.3.gz
	92.2K	Jan 10 15:00	/var/log/hostlogs/auth.log.1.gz
	92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.2.gz
	92.1K	Jan 4 17:30	/var/log/hostlogs/auth.log.3.gz
	92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.4.gz
	79.0K	Jan 12 01:59	/var/log/hostlogs/daemon.log.1.gz
	78.8K	Jan 11 23:15	/var/log/hostlogs/daemon.log.2.gz
	78.7K	Jan 11 20:30	/var/log/hostlogs/daemon.log.3.gz
	79.1K	Jan 11 17:44	/var/log/hostlogs/daemon.log.4.gz
	59.1K	Jan 11 21:59	/var/log/hostlogs/debug.1.gz
	59.2K	Jan 11 17:44	/var/log/hostlogs/debug.2.gz
	59.2K	Jan 11 13:29	/var/log/hostlogs/debug.3.gz
	59.3K	Jan 11 09:14	/var/log/hostlogs/debug.4.gz
	186.6K	Oct 20 16:31	/var/log/hostlogs/kern.log.1.gz
	238.3K	Jan 11 23:15	/var/log/hostlogs/lcmd.log.1.gz
	238.4K	Jan 11 17:30	/var/log/hostlogs/lcmd.log.2.gz
	238.6K	Jan 11 11:45	/var/log/hostlogs/lcmd.log.3.gz
	238.5K	Jan 11 06:00	/var/log/hostlogs/lcmd.log.4.gz
	372.5K	Jan 11 17:00	/var/log/hostlogs/syslog.1.gz
	372.5K	Jan 11 04:45	/var/log/hostlogs/syslog.2.gz
	371.9K	Jan 10 16:30	/var/log/hostlogs/syslog.3.gz
	372.7K	Jan 10 04:15	/var/log/hostlogs/syslog.4.gz
	10.1K	Jan 12 02:03	/var/log/messages.0.gz
	55.1K	Jan 6 21:25	/var/log/messages.1.gz
	81.5K	Dec 1 21:30	/var/log/messages.2.gz

```
Delete these files ? [yes,no] (no)
```


request system zeroize

Syntax request system zeroize
 <media>
 <local>

Release Information Command introduced before Junos OS Release 9.0.
 Command introduced in Junos OS Release 11.2 for EX Series switches.
 Option **media** added in Junos OS Release 11.4 for EX Series switches.
 Command introduced in Junos OS Release 12.2 for MX Series routers.
 Command introduced in Junos OS Release 12.3 for the QFX Series.
 Option **local** added in Junos OS Release 14.1.
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description



NOTE: The **media** option is not available on the QFX Series.

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to all Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as **root** and start the Junos OS CLI by typing **cli** at the prompt.



NOTE: If you configure the **commit synchronize** statement at the **[edit system]** hierarchy level and issue a **commit** in the master Routing Engine, the master configuration is automatically synchronized with the backup. However, if the backup Routing Engine is down when you issue the **commit**, the Junos OS displays a warning and commits the candidate configuration in the master Routing Engine. When the backup Routing Engine comes up, its configuration will automatically be synchronized with the master. A newly inserted backup Routing Engine automatically synchronizes its configuration with the master Routing Engine configuration.

To completely erase user-created data so that it is unrecoverable, use the **media** option.

Options **media**—(Optional) In addition to removing all configuration and log files, causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and so on. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the **request system zeroize media**

operation can take considerably more time than the **request system zeroize** operation. However, the critical security parameters are all removed at the beginning of the process.

local—(Optional) Remove all the configuration information and restore all the key values on the active Routing Engine.

Required Privilege Level maintenance

Related Documentation

- [request system snapshot on page 322](#)
- *Reverting to the Default Factory Configuration for the EX Series Switch*
- *Reverting to the Rescue Configuration for the EX Series Switch*
- *Reverting to the Default Factory Configuration*
- [Reverting to the Rescue Configuration on page 186](#)
- [Reverting to the Default Factory Configuration by Using the request system zeroize Command on page 185](#)

List of Sample Output [request system zeroize on page 378](#)
[request system zeroize media on page 379](#)

Sample Output

request system zeroize

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

0 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 5d19h20m26s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Mar 11 2011 - 04:39:06)

Board: EX4200-24T 2.11
EPLD: Version 6.0 (0x85)
DRAM: Initializing (1024 MB)
FLASH: 8 MB

Firmware Version: --- 01.00.00 ---
USB: scanning bus for devices... 2 USB Device(s) found
      scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.4
(user@host, Fri Mar 11 03:03:36 UTC 2011)
Memory: 1024MB
bootsequencing is enabled
```

```

bootsuccess is set
new boot device = disk0s1:
Loading /boot/defaults/loader.conf
/kernel data=0x915c84+0xa1260 syms=[0x4+0x7cbd0+0x4+0xb1c19]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
JUNOS 11.1R1.8 #0: 2011-03-09 20:14:25 UTC
    user@host:/volume/build/junos/11.1/release/11.1R1.8/obj-powerpc/bsd/kernels/
    JUNIPER-EX/kernel
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080
...

```

request system zeroize media

```

user@host> request system zeroize media
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing fpc0

{master:0}
root> Waiting (max 60 seconds) for system process `vnlr' to stop...done
...
Syncing disks, vnodes remaining...2 4 2 4 3 2 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 14m50s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD: Version 8.0 (0x82)
DRAM: Initializing (512 MB)
FLASH: 8 MB
NAND: No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
USB: scanning bus for devices... 2 USB Device(s) found
      scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2

```

```

(user@pool27.device.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
user@device.net:/volume/build/device/11.4/release/11.4R1.2/obj/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HID0 80004080<EMCP,TBEN,EN_MAS7_UPDATE>
real memory = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
. . .
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s2a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20055 free (31 frags, 2503 blocks, 0.0% fragmentation)
zeroizing /dev/da0s1a ...
. . .
zeroizing /dev/da0s3d ...
. . .
zeroizing /dev/da0s3e ...
. . .
zeroizing /dev/da0s4d ...
. . .
zeroizing /dev/da0s4e ...
. . .

syncing disks... All buffers synced.
Uptime: 3m40s
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)

Board: EX4200-48PX 1.1
EPLD: Version 8.0 (0x82)
DRAM: Initializing (512 MB)
FLASH: 8 MB
NAND: No NAND device found!!!
0 MiB

Firmware Version: --- 01.00.00 ---
USB: scanning bus for devices... 2 USB Device(s) found
      scanning bus for storage devices... 1 Storage Device(s) found

```

```

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(user@device.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
user@device.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/
bsd/kernels/JUNIPER-EX/kernel
can't re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: H1D0 80004080 <EMCP,TBEN,EN_MAS7_UPDATE>
real memory = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
...
Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s1a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20064 free (48 frags, 2502 blocks, 0.1% fragmentation)
zeroizing /dev/da0s2a ...
...
Creating initial configuration...mgd: error: Cannot open configuration file:
/config/juniper.conf
mgd: warning: activating factory configuration
mgd: commit complete
mgd: -----
mgd: Please login as 'root'. No password is required.
mgd: To start Initial Setup, type 'ezsetup' at the JUNOS prompt.
mgd: To start JUNOS CLI, type 'cli' at the JUNOS prompt.
mgd: -----
Setting initial options: debugger_on_panic=NO debugger_on_break=NO.
Starting optional daemons: .
Doing initial network setup:
...

Amnesiac (ttyu0)

```

show chassis usb storage

Syntax	show chassis usb storage
Release Information	Command introduced in Junos OS Release 11.4 R2.
Description	Display the current status of any USB mass storage device and whether the USB ports are enabled or disabled.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 68
List of Sample Output	show chassis hardware detail on page 382 show chassis usb storage on page 382

Sample Output

show chassis hardware detail

```

user@host> show chassis hardware detail
Hardware inventory:
Item              Version  Part number  Serial number  Description
Chassis
Routing Engine    REV 01   750-043613   BV4911AA0005   SRX240H2-POE
usb0 (addr 1)     DWC OTG root hub 0   vendor 0x0000   uhub0
usb0 (addr 2)     product 0x005a 90   vendor 0x0409   uhub1
usb0 (addr 3)     ST72682 High Speed Mode 64218 STMicroelectronics umass0
usb0 (addr 4)     Mass Storage Device 4096 JetFlash   umass1
FPC 0
PIC 0
Power Supply 0
FPC
16x GE Base PIC

```

show chassis usb storage

```

user@host> show chassis usb storage
USB Disabled

```

show system autoinstallation status

Syntax	show system autoinstallation status
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command supported in Junos OS Release 12.2 for ACX Series Universal Access Routers.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	(ACX Series routers, and EX Series switches only) Display autoinstallation status information.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>ACX Series Autoinstallation Overview</i> • <i>Before You Begin Autoinstallation on an ACX Series Universal Access Router</i> • <i>Autoinstallation Configuration of ACX Series Universal Access Routers</i> • <i>USB Autoinstallation on ACX Series Routers</i> • <i>Autoinstalling a Configuration File from a Disk-on-Key USB Memory Stick onto an EX2200 or EX3300 Switch</i> • <i>Verifying Autoinstallation on ACX Series Universal Access Routers</i> • <i>autoinstallation</i>
List of Sample Output	show system autoinstallation status on page 384
Output Fields	Table 47 describes the output fields for the show system autoinstallation status command. Output fields are listed in the approximate order in which they appear.

Table 47: show system autoinstallation status Output Fields

Field Name	Field Description
Autoinstallation status	<p>Display autoinstallation status information:</p> <ul style="list-style-type: none"> • Last committed file—File last committed for autoinstallation configuration. • Configuration server of last committed file—IP address or URL of the server configured to retrieve configuration information for the last committed configuration file. • Interface—Interface configured for autoinstallation. <ul style="list-style-type: none"> • Name—Name of the interface. • State—Interface state. • Address acquisition—Display IP address acquired and protocol used for acquisition upon startup. <ul style="list-style-type: none"> • Protocol—Protocol used for acquisition: BOOTP/DHCP or RARP. • Acquired address—IP address acquired from the DHCP server.

Sample Output

show system autoinstallation status

```
user@host> show system autoinstallation status
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 0.0.0.0
Interface:
  Name: ge-0/0/1
  State: None
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```


show system autorecovery state

Syntax	show system autorecovery state
Release Information	Command introduced in Junos OS Release 11.2.
Description	Perform checks and show status of all autorecovered items.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system autorecovery state on page 292 • Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 169
List of Sample Output	show system autorecovery state on page 385
Output Fields	Table 48 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear.

Table 48: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state
```

```
Configuration:
File          Recovery Information Integrity Check Action / Status
rescue.conf.gz Saved          Passed          None
Licenses:
File          Recovery Information Integrity Check Action / Status
JUNOS282736.lic Saved          Passed          None
JUNOS282737.lic Not Saved      Not checked     Requires save
BSD Labels:
Slice         Recovery Information Integrity Check Action / Status
s1            Saved          Passed          None
s2            Saved          Passed          None
```

s3	Saved	Passed	None
s4	Saved	Passed	None

show system boot-messages

List of Syntax	Syntax on page 387 Syntax (EX Series Switches) on page 387 Syntax (TX Matrix Router) on page 387 Syntax (TX Matrix Plus Router) on page 387 Syntax (MX Series Router) on page 387 Syntax (QFX Series) on page 387
Syntax	show system boot-messages
Syntax (EX Series Switches)	show system boot-messages <all-members> <local> <member <i>member-id</i> >
Syntax (TX Matrix Router)	show system boot-messages <all-chassis all-lcc lcc <i>number</i> scc>
Syntax (TX Matrix Plus Router)	show system boot-messages <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> >
Syntax (MX Series Router)	show system boot-messages <all-members> <local> <member <i>member-id</i> >
Syntax (QFX Series)	show system boot-messages infrastructure <i>name</i> interconnect-device <i>name</i> node-group <i>name</i>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display initial messages generated by the system kernel upon startup. These messages are the contents of <code>/var/run/dmesg.boot</code> .
Options	none —Display all boot time messages. all-chassis —(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display boot time messages for all of the chassis. all-lcc —(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for all T640 routers connected to a TX Matrix router. On a TX Matrix Plus router, display boot time messages for all connected T1600 or T4000 LCCs. all-members —(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on all members of the Virtual Chassis configuration.

infrastructure *name*—(QFabric systems only) (Optional) Display boot time messages on the fabric control Routing Engine or fabric manager Routing engines.

interconnect-device *name*—(QFabric systems only) (Optional) Display boot time messages on the Interconnect device.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for a specific T640 router connected to a TX Matrix router. On a TX Matrix Plus router, display boot time messages for a specific router connected to a TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the local Virtual Chassis member.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

node-group *name*—(QFabric systems only) (Optional) Display boot time messages on the Node group.

scc—(TX Matrix routers only) (Optional) Display boot time messages for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Display boot time messages for the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system boot-messages** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output

[show system boot-messages \(TX Matrix Router\) on page 389](#)
[show system boot-messages lcc \(TX Matrix Router\) on page 390](#)
[show system boot-messages \(TX Matrix Plus Router\) on page 391](#)
[show system boot-messages \(QFX3500 Switch\) on page 391](#)

Sample Output

show system boot-messages (TX Matrix Router)

```
user@host> show system boot-messages
Copyright (c) 1992-1998 FreeBSD Inc.
Copyright (c) 1996-2000 Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California. All rights reserved.

JUNOS 4.1-20000216-Zf8469 #0: 2000-02-16 12:57:28 UTC
    tlim@device1.example.com:/p/build/20000216-0905/4.1/release_kernel/sys/compile/GENERIC
CPU: Pentium Pro (332.55-MHz 686-class CPU)
    Origin = "GenuineIntel" Id = 0x66a Stepping=10
    Features=0x183f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,<b
16>,<b17>,MMX,<b24>>
Teknor CPU Card Recognized
real memory = 805306368 (786432K bytes)
avail memory = 786280448 (767852K bytes)
Probing for devices on PCI bus 0:
chip0 <generic PCI bridge (vendor=8086 device=7192 subclass=0)> rev 3 class 6000
0 on pci0:0:0
chip1 <Intel 82371AB PCI-ISA bridge> rev 1 class 60100 on pci0:7:0
chip2 <Intel 82371AB IDE interface> rev 1 class 10180 on pci0:7:1
chip3 <Intel 82371AB USB interface> rev 1 class c0300 int d irq 11 on pci0:7:2
smb0 <Intel 82371AB SMB controller> rev 1 class 68000 on pci0:7:3
pcic0 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int a irq 15 on pci0:13
:0
TI1131 PCI Config Reg: [pci only][FUNC0 pci int]
pcic1 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int b irq 12 on pci0:13
:1
TI1131 PCI Config Reg: [pci only][FUNC1 pci int]
fxp0 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 12 on

pci0:16:0
chip4 <generic PCI bridge (vendor=1011 device=0022 subclass=4)> rev 4 class 6040
0 on pci0:17:0
fxp1 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on

pci0:19:0
Probing for devices on PCI bus 1:
mcs0 <Miscellaneous Control Subsystem> rev 12 class ff0000 int a irq 12 on pci1:
13:0
fxp2 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on

pci1:14:0
Probing for devices on the ISA bus:
sc0 at 0x60-0x6f irq 1 on motherboard
sc0: EGA color <16 virtual consoles, flags=0x0>
ed0 not found at 0x300
```

```

ed1 not found at 0x280
ed2 not found at 0x340
psm0 not found at 0x60
sio0 at 0x3f8-0x3ff irq 4 flags 0x20010 on isa
sio0: type 16550A, console
sio1 at 0x3e8-0x3ef irq 5 flags 0x20000 on isa
sio1: type 16550A
sio2 at 0x2f8-0x2ff irq 3 flags 0x20000 on isa
sio2: type 16550A
pcic0 at 0x3e0-0x3e1 on isa
PC-Card ctlr(0) TI PCI-1131 [CardBus bridge mode] (5 mem & 2 I/O windows)
pcic0: slot 0 controller I/O address 0x3e0
npx0 flags 0x1 on motherboard
npx0: INT 16 interface
fdc0: direction bit not set
fdc0: cmd 3 failed at out byte 1 of 3
fdc0 not found at 0x3f0
wdc0 at 0x1f0-0x1f7 irq 14 on isa
wdc0: unit 0 (wd0): <SunDisk SQFXB-80>, single-sector-i/o
wd0: 76MB (156672 sectors), 612 cyls, 8 heads, 32 S/T, 512 B/S
wdc0: unit 1 (wd1): <IBM-DCXA-210000>
wd1: 8063MB (16514064 sectors), 16383 cyls, 16 heads, 63 S/T, 512 B/S
wdc1 not found at 0x170
wdc2 not found at 0x180
ep0 not found at 0x300
fxp0: Ethernet address 00:a0:a5:12:05:5a
fxp1: Ethernet address 00:a0:a5:12:05:59
fxp2: Ethernet address 02:00:00:00:00:01
swapon: adding /dev/wd1s1b as swap device
Automatic reboot in progress...
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd0s1e: clean, 9233 free (9 frags, 1153 blocks, 0.1% fragmentation)
/dev/rwd0s1a: clean, 16599 free (95 frags, 2063 blocks, 0.1% fragmentation)
/dev/rwd1s1f: clean, 4301055 free (335 frags, 537590 blocks, 0.0% fragmentation)

```

show system boot-messages lcc (TX Matrix Router)

```

user@host> show system boot-messages lcc 2
lcc2-re0:
-----
Copyright (c) 1996-2001, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2001 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
JUNOS 7.0-20040912.0 #0: 2004-09-12 09:16:32 UTC

builder@device1.example.com:/build/benten-b/7.0/20040912.0/obj-i386/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz
Timecounter "TSC" frequency 601368936 Hz
CPU: Pentium III/Pentium III Xeon/Celeron (601.37-MHz 686-class CPU)
    Origin = "GenuineIntel" Id = 0x68a Stepping = 10

Features=0x387f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,PN,MMX,FXSR,SSE>
real memory = 2147467264 (2097136K bytes)
sio0: gdb debugging port
avail memory = 2084040704 (2035196K bytes)
Preloaded elf kernel "kernel" at 0xc06d9000.
DEVFS: ready for devices
Pentium Pro MTRR support enabled
md0: Malloc disk

```

```

DRAM Data Integrity Mode: ECC Mode with h/w scrubbing
npx0: <math processor> on motherboard
npx0: INT 16 interface
pcib0: <ServerWorks NB6635 3.0LE host to PCI bridge> on motherboard
pci0: <PCI bus> on pcib0
pcic-pci0: <TI PCI-1410 PCI-CardBus Bridge> irq 15 at device 1.0 on pci0
pcic-pci0: TI12XX PCI Config Reg: [pwr save][pci only]
fxp0: <Intel Embedded 10/100 Ethernet> port 0x1000-0x103f mem
0xfb800000-0xfb81ffff,0xfb820000-0xfb820fff irq 9 at device 3.0 on pci0
fxp1: <Intel Embedded 10/100 Ethernet> port 0x1040-0x107f mem
0xfb840000-0xfb85ffff,0xfb821000-0xfb821fff irq 11 at device 4.0 on pci0
...

```

show system boot-messages (TX Matrix Plus Router)

```

user@host> show system boot-messages
sfc0-re0:
-----
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
JUNOS 9.6B3.3 #0: 2009-06-17 19:52:08 UTC

builder@device1.example.com:/volume/build/junos/9.6/release/9.6B3.3/obj-i386/bsd/sys/compile/JUNIPER
MPTable: Timecounter "i8254" frequency 1193182 Hz quality 0 CPU: Intel(R) Xeon(R)
CPU          L5238 @ 2.66GHz (2660.01-MHz 686-class CPU)   Origin =
"GenuineIntel" Id = 0x1067a Stepping = 10   Features=0xbfebfbff
...
lcc1-re0:
-----
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
JUNOS 9.6-20090617.0 #0: 2009-06-17 04:15:14 UTC

builder@device1.example.com:/volume/build/junos/9.6/production/20090617.0/obj-i386/bsd/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Xeon(R) CPU                               @ 1.86GHz (1862.01-MHz 686-class CPU)

Origin = "GenuineIntel" Id = 0x1067a Stepping = 10
Features=0xbfebfbff
...

```

show system boot-messages (QFX3500 Switch)

```

user@switch> show sytem boot-messages
getmemsize: msgbufp[size=32768] = 0x81d07fe4

System physical memory distribution:
-----
Total physical memory: 4160749568 (3968 MB)
Physical memory used: 3472883712 (3312 MB)
Physical memory allocated to kernel: 2130706432 (2032 MB)
Physical memory allocated to user BTLB: 1342177280 (1280 MB)
-----

Copyright (c) 1996-2010, Juniper Networks, Inc.

```

```

All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.
JUNOS 11.1I #0: 2010-09-17 19:18:07 UTC
    user@device1.example.com:/c/user/DEV_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
WARNING: debug.mpsafenet forced to 0 as ipsec requires Giant
JUNOS 11.1I #0: 2010-09-17 19:18:07 UTC
    user@device.net:/c/test/DEV_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
real memory = 3472883712 (3312MB)
avail memory = 1708171264 (1629MB)
cpuid: 0, btlb_cpumap:0xffffffff8
FreeBSD/SMP: Multiprocessor System Detected: 12 CPUs
ETHERNET SOCKET BRIDGE initialising
Initializing QFX platform properties ..
cpu0 on motherboard
: RMI's XLR CPU Rev. 0.3 with no FPU implemented
    L1 Cache: I size 32kb(32 line), D size 32kb(32 line), eight way.
    L2 Cache: Size 1024kb, eight way
pic_lbus0: <XLR Local Bus>
pic_lbus0: <XLR Local Bus> on motherboard
Enter qfx control ethernet probe addr:0xc5eeec00
gmac4: <XLR GMAC GE Ethernet> on pic_lbus0
me0: Ethernet address 00:1d:b5:f7:68:40
Enter qfx control ethernet probe addr:0xc5eeeb40
gmac5: <XLR GMAC GE Ethernet> on pic_lbus0
me1: Ethernet address 00:1d:b5:f7:68:41
Enter qfx control ethernet probe addr:0xc5eeea80
gmac6: <XLR GMAC GE Ethernet> on pic_lbus0
me1: Ethernet address 00:1d:b5:f7:68:42
sio0 on pic_lbus0
Entering sioattach
sio0: type 16550A, console
xls_setup_intr: skip irq 3, xlr regs are set up somewhere else.
gblmem0 on pic_lbus0
ehci0: <RMI XLS USB 2.0 controller> on pic_lbus0
ehci_bus_attach: allocated resource. tag=1, base=bef24000
xls_ehci_init: endian hardware swapping NOT enabled.
usb0: EHCI version 1.0
usb0 on ehci0
usb0: USB revision 2.0
uhub0: vendor 0x0000 EHCI root hub, class 9/0, rev 2.00/1.00, addr 1
uhub0: 2 ports with 2 removable, self powered
umass0: USB USBFlashDrive, rev 2.00/11.00, addr 2
pcib0: PCIe link 0 up
pcib0: PCIe link 2 up
pcib0: PCIe link 3 up
pcib0: <XLS PCI Host Controller> on pic_lbus0
pci0: <PCI bus> on pcib0
pcib1: <PCI-PCI bridge> at device 0.0 on pci0
pci1: <PCI bus> on pcib1
pci1: <network, ethernet> at device 0.0 (no driver attached)
pcib2: <PCI-PCI bridge> at device 1.0 on pci0
pcib3: <PCI-PCI bridge> at device 2.0 on pci0
pci2: <PCI bus> on pcib3
pci2: <network, ethernet> at device 0.0 (no driver attached)
pcib4: <PCI-PCI bridge> at device 3.0 on pci0
pci3: <PCI bus> on pcib4
pci3: <network, ethernet> at device 0.0 (no driver attached)

```



```

cfi device address space at 0xbc000000
cfi0: <AMD/Fujitsu - 8MB> on pic_lbus0
cfi device address space at 0xbc000000
i2c0: <I2C bus controller> on pic_lbus0
i2c1: <I2C bus controller> on pic_lbus0
qfx_fmn0 on pic_lbus0
pool offset 1503776768
xlr_lbus0: <XLR Local Bus Controller> on motherboard
qfx_bcpld_probe[124]
qfx_bcpld_probe[138]: dev_type=0x0
qfx_bcpld_probe[124]
qfx_bcpld0: QFX BCPLD probe success
qfx_bcpld0qfx_bcpld_attach[174]
qfx_bcpld_attach[207] : bus_space_tag=0x0, bus_space_handle=0xbd900000
qfx_bcpld_probe[124]
qfx_bcpld1: QFX BCPLD probe success
qfx_bcpld1qfx_bcpld_attach[174]
tor_bcpld_slave_attach[1245] : bus_space_tag=0x0, bus_space_handle=0xbda00000
Initializing product: 96 ..
bmeb: bmeb_lib_init done 0xc60a5000, addr 0x809c99a0
bme0:Virtual BME driver initializing
Timecounter "mips" frequency 1200000000 Hz quality 0
Timecounter "xlr_pic_timer" frequency 66666666 Hz quality 1
Timecounters tick every 1.000 msec
Loading the NETPFE fc module
IPsec: Initialized Security Association Processing.
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #7 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #11 Launched!
SMP: AP CPU #10 Launched!
SMP: AP CPU #9 Launched!
SMP: AP CPU #8 Launched!
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <USB USBFlashDrive 1100> Removable Direct Access SCSI-0 device
da0: 40.000MB/s transfers
da0: 3920MB (8028160 512 byte sectors: 255H 63S/T 499C)
Trying to mount root from ufs:/dev/da0s1a

```

show system auto-snapshot

Syntax	show system auto-snapshot
Release Information	Command introduced in Junos OS Release 12.3 for EX Series switches. Command introduced in Junos OS Release 12.1X45-D10 for SRX Series devices.
Description	Display automatic snapshot status information. When the automatic snapshot feature is enabled and the system reboots from the alternate root partition, the switch automatically takes a snapshot of the root file system in the alternate root partition and copies it onto the primary root partition. This automatic snapshot procedure takes place whenever the system reboots from the alternate partition, regardless of whether the reboot from the alternate partition is due to a command or due to a corruption of the primary partition.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Understanding Resilient Dual-Root Partitions on Switches on page 95
List of Sample Output	show system auto-snapshot on page 395
Output Fields	Table 49 describes the output fields for the show system auto-snapshot command. Output fields are listed in the approximate order in which they appear.

Table 49: show system auto-snapshot status Output Fields

Field Name	Field Description
Auto-snapshot configuration	<p>Status of the configuration:</p> <ul style="list-style-type: none"> • Enabled—If the system reboots from the alternate partition, the automatic snapshot feature automatically takes a snapshot of the alternate partition and copies it onto the primary partition. • Disabled—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, request system snapshot, to take a snapshot of one partition and copy it onto the other.
Auto-snapshot state	<p>Status of the automatic snapshot procedure:</p> <ul style="list-style-type: none"> • Completed—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared. • Disabled—The automatic snapshot procedure is inactive. • In progress—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size.

Sample Output

show system auto-snapshot

```
user@switch> show system auto-snapshot
Auto-snapshot Configuration: Enabled
Auto-snapshot State: Disabled
```

show system download

Syntax	<code>show system download <download-id></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Display a brief summary of all the download instances along with their current state and extent of progress. If a download-id is provided, the command displays a detailed report of the particular download instance.
Options	<ul style="list-style-type: none"> download-id—(Optional) The ID number of the download instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> request system download start on page 298 Understanding Download Manager for SRX Series Devices on page 51 Understanding Download Manager for EX Series Devices
List of Sample Output	show system download on page 396 show system download 1 on page 397
Output Fields	Table 50 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear.

Table 50: show system download Output Fields

Field Name	Field Description
ID	Displays the download identification number.
Status	Displays the state of a particular download.
Start Time	Displays the start time of a particular download.
Progress	Displays the percentage of a download that has been completed.
URL	Displays the URL from which the file was downloaded.

Sample Output

show system download

```

user@host> show system download
Download Status Information:
ID  Status  Start Time      Progress  URL
1   Active   May 4 06:28:36  5%        ftp://ftp-server//tftpboot/1m_file
2   Active   May 4 06:29:07  3%        ftp://ftp-server//tftpboot/5m_file
3   Error    May 4 06:29:22  Unknown   ftp://ftp-server//tftpboot/badfile

```

4 Completed May 4 06:29:40 100% ftp://ftp-server//tftpboot/smallfile

show system download 1

```
user@host> show system download 1
```

```
Download ID      : 1
Status           : Active
Progress         : 6%
URL              : ftp://ftp-server//tftpboot/1m_file
Local Path       : /var/tmp/1m_file
Maximum Rate     : 1k
Creation Time    : May 4 06:28:36
Scheduled Time   : May 4 06:28:36
Start Time       : May 4 06:28:37
Error Count      : 0
```

show system license

Syntax	show system license <installed keys usage>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 13.3 for the MX104 3D Universal Edge Routers.
Description	Display licenses and information about how they are used.
Options	<p>none—Display all license information.</p> <p>installed—(Optional) Display installed licenses only.</p> <p>keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p>usage—(Optional) Display the state of licensed features.</p>
Required Privilege Level	maintenance
List of Sample Output	show system license on page 399 show system license installed on page 400 show system license keys on page 400 show system license usage on page 400 show system license (MX104 Routers) on page 400 show system license installed (MX104 Routers) on page 401 show system license keys (MX104 Routers) on page 401 show system license usage (MX104 Routers) on page 401 show system license (MX104 Routers) on page 401 show system license installed (MX104 Routers) on page 402 show system license keys (MX104 Routers) on page 402 show system license usage (MX104 Routers) on page 403 show system license (MX104 Routers) on page 403 show system license installed (MX104 Routers) on page 403 show system license keys (MX104 Routers) on page 404 show system license usage (MX104 Routers) on page 404 show system license (QFX Series) on page 404 show system license (QFX5110 Switch with Disaggregated Feature License) on page 404
Output Fields	Table 51 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear. <i>Reviewer: Anything more I should add for disaggregated licenses below?</i>

Table 51: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	<p>Number of licenses used by a router or switch. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.</p> <p>NOTE: In Junos OS Release 10.1 and later, the Licenses used column displays the actual usage count based on the number of active sessions or connections as reported by the corresponding feature daemons. This is applicable for scalable license-based features such as Subscriber Access (scale-subscriber), L2TP (scale-l2tp), Mobile IP (scale-mobile-ip), and so on.</p>
Licenses installed	<p>Information about the installed license key:</p> <ul style="list-style-type: none"> • License identifier—Identifier associated with a license key. • State—State of the license key: valid or invalid. An invalid state indicates that the key was entered incorrectly or is not valid for the specific device. • License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • Software Serial Number—Serial number of the disaggregated software feature license. License Management System (LMS) uses the software serial number, not the chassis ID, to generate a disaggregated feature license. • Customer ID—what is this exactly? • Valid for device—Device that can use a license key. • Group defined—Group membership of a device. • Features—Feature associated with a license, such as data link switching (DLSw).
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Amount of time left within the grace period before a license is required for a feature being used.

Sample Output

show system license

```
user@host> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
subscriber-accounting	2	2	0	permanent
subscriber-authentication	1	2	0	permanent
subscriber-address-assignment	2	2	0	permanent
subscriber-vlan	2	2	0	permanent
subscriber-ip	0	2	0	permanent
scale-subscriber	2	3	0	permanent
scale-l2tp	4	5	0	permanent
scale-mobile-ip	1	2	0	permanent

```
Licenses installed:
```

```
License identifier: XXXXXXXXXX
```

```
License version: 2
```

Features:

```

subscriber-accounting - Per Subscriber Radius Accounting
    permanent
subscriber-authentication - Per Subscriber Radius Authentication
    permanent
subscriber-address-assignment - Radius/SRC Address Pool Assignment
    permanent
subscriber-vlan - Dynamic Auto-sensed Vlan
    permanent
subscriber-ip - Dynamic and Static IP
    permanent

```

show system license installed

```

user@host> show system license installed
License identifier: XXXXXXXXXX
License version: 2
Features:
subscriber-accounting - Per Subscriber Radius Accounting
    permanent
subscriber-authentication - Per Subscriber Radius Authentication
    permanent
subscriber-address-assignment - Radius/SRC Address Pool Assignment
    permanent
subscriber-vlan - Dynamic Auto-sensed Vlan
    permanent
subscriber-ip - Dynamic and Static IP
    permanent

```

show system license keys

```

user@host> show system license keys
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxx

```

show system license usage

```

user@host> show system license usage
License usage:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
subscriber-accounting	2	2	0	permanent
subscriber-authentication	1	2	0	permanent
subscriber-address-assignment	2	2	0	permanent
subscriber-vlan	2	2	0	permanent
subscriber-ip	0	2	0	permanent
scale-subscriber	2	3	0	permanent
scale-l2tp	4	5	0	permanent
scale-mobile-ip	1	2	0	permanent

show system license (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

```

user@host> show system license
License usage:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
scale-subscriber	0	1000	0	permanent

scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent
MX104-2x10Gig-port-0-1	0	1	0	permanent

Licenses installed:

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)

upgrade

permanent

show system license installed (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

user@host > show system license installed

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)

upgrade

permanent

show system license keys (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

user@host > show system license keys

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 0 and 1 are activated by installing the license to activate the first two built-in ports.

user@host > show system license usage

Feature name	Licenses used	Licenses installed	Expiry	needed	
scale-subscriber	0	1000		0	permanent
scale-l2tp	0	1000		0	permanent
scale-mobile-ip	0	1000		0	permanent
MX104-2x10Gig-port-0-1	0	1		0	permanent

show system license (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

user@host > show system license

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
scale-subscriber	0	1000	0	permanent

scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent
MX104-2x10Gig-port-0-1	0	1	0	permanent
MX104-2x10Gig-port-2-3	0	1	0	permanent

Licenses installed:

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)

upgrade

permanent

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)

upgrade

permanent

show system license installed (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

user@host > show system license installed

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)

upgrade

permanent

License identifier: XXXXXXXXXX

License version: 2

Features:

MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)

upgrade

permanent

show system license keys (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

user@host > show system license keys

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxx
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxx
```

show system license usage (MX104 Routers)

In the following output, ports 2 and 3 are activated by installing the license to activate the next two built-in ports after installing the license to activate the first two built-in ports.

```
user@host > show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
scale-subscriber	0	1000	0	permanent
scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent
MX104-2x10Gig-port-0-1	0	1	0	permanent
MX104-2x10Gig-port-2-3	0	1	0	permanent

show system license (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
scale-subscriber	0	1000	0	permanent
scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent
MX104-2x10Gig-port-0-1	0	1	0	permanent
MX104-2x10Gig-port-2-3	0	1	0	permanent

```
Licenses installed:
License identifier: XXXXXXXXXX
License version: 2
Features:
  MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
  permanent
  MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
  permanent
```

show system license installed (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license installed
```

License identifier: XXXXXXXXXX

License version: 2

Features:

```
  MX104-2x10Gig-port-0-1 - MX104 2X10Gig Builtin Port(xe-2/0/0 & xe-2/0/1)
upgrade
  permanent
  MX104-2x10Gig-port-2-3 - MX104 2X10Gig Builtin Port(xe-2/0/2 & xe-2/0/3)
upgrade
  permanent
```

show system license keys (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license keys
```

```
XXXXXXXX XXXXXX XXXXXX XXXXXX XXXXXX XXXXXX
XXXXXXXX XXXXXX XXXXXX XXXXXX XXXXXX
XXXXXXXX XXXXXX X
```

show system license usage (MX104 Routers)

In the following output, ports 0,1,2, and 3 are activated by installing a single license key to activate all four built-in ports.

```
user@host > show system license usage
```

Feature name	Licenses used	Licenses installed	Expiry needed	
scale-subscriber	0	1000	0	permanent
scale-l2tp	0	1000	0	permanent
scale-mobile-ip	0	1000	0	permanent
MX104-2x10Gig-port-0-1	0	1	0	permanent
MX104-2x10Gig-port-2-3	0	1	0	permanent

show system license (QFX Series)

```
user@switch> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
qfx-edge-fab	1	1	1	permanent

Licenses installed:

License identifier: JUNOS417988

License version: 1

Features:

```
qfx-edge-fab - QFX3000 Series QF/Node feature license
permanent
```

show system license (QFX5110 Switch with Disaggregated Feature License)

```
user@switch> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp	0	1	0	2017-07-05
00:00:00 UTC				
isis	0	1	0	2017-07-05
00:00:00 UTC				
vxlان	0	1	0	2017-07-05
00:00:00 UTC				
ovsdb	0	1	0	2017-07-05
00:00:00 UTC				
jbs1	0	1	0	2017-07-02
00:00:00 UTC				
upgrade1	0	1	0	2017-07-05
00:00:00 UTC				

Licenses installed:

License identifier: JUNOS797095

```
License version: 4
Software Serial Number: 91730A00223925
Customer ID: Juniper
Features:
  JUNOS-BASE-SERVICES-CLASS-1 - QFX Junos Base Services license for Class 1 HW
    date-based, 2016-07-01 00:00:00 UTC - 2017-07-02 00:00:00 UTC

License identifier: JUNOS797646
License version: 4
Software Serial Number: 91730A00224207
Customer ID: Juniper
Features:
  CLASS-1-JUNOS-BASE-ADVANCED-UPGRADE - Class 1 Junos Base to Advanced Services
  Upgrade
    date-based, 2016-07-04 00:00:00 UTC - 2017-07-05 00:00:00 UTC

{master:0}
```

show system license (View)

Syntax	show system license <installed keys status usage>
Release Information	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
Description	Display licenses and information about how licenses are used.
Options	<p>none—Display all license information.</p> <p>installed—(Optional) Display installed licenses only.</p> <p>keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p>status—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p>usage—(Optional) Display the state of licensed features.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Working with License Keys for SRX Series Devices</i>
List of Sample Output	<p>show system license on page 407</p> <p>show system license installed on page 407</p> <p>show system license keys on page 408</p> <p>show system license usage on page 408</p> <p>show system license status logical-system all on page 408</p>
Output Fields	Table 52 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 52: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.

Table 52: show system license Output Fields (*continued*)

Field Name	Field Description
Licenses installed	Information about the installed license key: <ul style="list-style-type: none"> • License identifier—Identifier associated with a license key. • License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • Valid for device—Device that can use a license key. • Features—Feature associated with a license.
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Time remaining in the grace period before a license is required for a feature being used.
Logical system license status	Displays whether a license is enabled for a logical system.

Sample Output

show system license

```
user@host> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

```
Licenses installed:
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys
```

```
XXXXXXXXXX xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxx
```

show system license usage

```
user@host> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:
```

logical system name	license status
root-logical-system	enabled
LSYS0	enabled
LSYS1	enabled
LSYS2	enabled

show system login logout

Syntax	show system login logout
Release Information	Command introduced in Junos OS Release 11.2.
Description	Display the usernames locked after unsuccessful login attempts.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> • lockout-period on page 1244 • clear system login logout on page 291
List of Sample Output	show system login logout on page 409
Output Fields	Table 53 lists the output fields for the show system login logout command. Output fields are listed in the approximate order in which they appear.

Table 53: show system login logout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

Sample Output

show system login logout

```
user@host> show system login logout
```

```

User                Lockout start          Lockout end
root                2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC

```

show system snapshot

List of Syntax [Syntax on page 410](#)
 [Syntax \(EX Series Switches\) on page 410](#)

Syntax show system snapshot

Syntax (EX Series Switches) show system snapshot
 <all-members|local|member *member-id*>
 <media (external | internal)>

Release Information Command introduced in Junos OS Release 7.6.
 Command introduced in Junos OS Release 10.0 for EX Series switches.
 Option **slice** deprecated for Junos OS with Upgraded FreeBSD in Junos OS Release 15.1.



NOTE: To determine which platforms run Junos OS with Upgraded FreeBSD, see the table listing the platforms currently running Junos OS with upgraded FreeBSD in “[Understanding Junos OS with Upgraded FreeBSD](#)” on page 19.

Description Display information about the backup software:

- On the routers, display information about the backup software, which is located in the **/altroot**, and **/altconfig** file systems or on the alternate media.
- On the switches, display information about the backup of the root file system (**/**) and directories **/altroot**, **/config**, **/var**, and **/var/tmp**, which are located either on an external USB flash drive or in internal flash memory.



NOTE: To back up software, use the **request system snapshot** command.

Options **none**—Display information about the backup software.

all-members | local | member *member-id*—(EX Series switch Virtual Chassis only)
 (Optional) Display the snapshot in a Virtual Chassis:

- **all-members**—Display the snapshot for all members of the Virtual Chassis.
- **local**—Display the snapshot on the member of the Virtual Chassis that you are currently logged into.
- **member *member-id***—Display the snapshot for the specified member of the Virtual Chassis.

media (external | internal)—(EX Series switch only) (Optional) Display the destination media location for the snapshot. The **external** option specifies the snapshot on an external mass storage device, such as a USB flash drive. The **internal** option specifies

the snapshot on an internal memory source, such as internal flash memory. If no additional options are specified, the command displays the snapshot stored in both slices.

Required Privilege Level view

Related Documentation • [request system snapshot on page 322](#)

List of Sample Output [show system snapshot \(Router\) on page 411](#)
[show system snapshot media external \(Switch\) on page 411](#)
[show system snapshot media internal \(Switch\) on page 412](#)

Output Fields Table 54 lists the output fields for the **show system snapshot** command. Output fields are listed in the approximate order in which they appear.

Table 54: show system snapshot Output Fields

Field Name	Field Description
Creation date	Date and time of the last snapshot.
JUNOS version on snapshot	Junos OS release number of individual software packages.

Sample Output

show system snapshot (Router)

```
user@host> show system snapshot
Information for snapshot on hard-disk
Creation date: Oct 5 13:53:29 2005
JUNOS version on snapshot:
  jbase : 7.3R2.5
  jcrypto: 7.3R2.5
  jdocs : 7.3R2.5
  jkernel: 7.3R2.5
  jpfe : M40-7.3R2.5
  jroute : 7.3R2.5
```

show system snapshot media external (Switch)


```
user@switch> show system snapshot media external
Information for snapshot on external (/dev/dals1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on external (/dev/dals2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase : ex-12.2I20120305_2240_user
```

```
jcrypto-ex: 12.2I20120305_2240_user
jdocs-ex: 12.2I20120305_2240_user
jroute-ex: 12.2I20120305_2240_user
jswitch-ex: 12.2I20120305_2240_user
jweb-ex: 12.2I20120305_2240_user
```

show system snapshot media internal (Switch)

```
user@switch> show system snapshot media internal
Information for snapshot on internal (/dev/da0s1a) (backup)
Creation date: Mar 14 05:01:02 2011
JUNOS version on snapshot:
  jbase : 11.1R1.9
  jcrypto-ex: 11.1R1.9
  jdocs-ex: 11.1R1.9
  jkernel-ex: 11.1R1.9
  jroute-ex: 11.1R1.9
  jswitch-ex: 11.1R1.9
  jweb-ex: 11.1R1.9
  jpfe-ex42x: 11.1R1.9
Information for snapshot on internal (/dev/da0s2a) (primary)
Creation date: Mar 30 08:46:27 2011
JUNOS version on snapshot:
  jbase : 11.2-20110330.0
  jcrypto-ex: 11.2-20110330.0
  jdocs-ex: 11.2-20110330.0
  jkernel-ex: 11.2-20110330.0
  jroute-ex: 11.2-20110330.0
  jswitch-ex: 11.2-20110330.0
  jweb-ex: 11.2-20110330.0
  jpfe-ex42x: 11.2-20110330.0
```

show system snapshot (Junos OS with Upgraded FreeBSD)

Syntax	show system snapshot
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers and EX9200 switches. Command introduced in Junos OS Release 15.1X53-D30 for QFX5200 switches.
Description	Display information about the non-recovery backup software, which is located in the junos file system on the hard disk drive or solid-state drive (SSD).
<div>  NOTE: To back up software, use the request system snapshot command. </div>	
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system snapshot (Junos OS with Upgraded FreeBSD) on page 329 • request system reboot (Junos OS with Upgraded FreeBSD) on page 316 • Understanding Junos OS with Upgraded FreeBSD on page 19
List of Sample Output	show system snapshot on page 413
Output Fields	When you enter this command, you are provided feedback on the status of your request. If there are no snapshots available, the command returns null output.

Sample Output

show system snapshot

```
user@host> show system snapshot
Snapshot snap.20141219.122106:
Location: /packages/sets/snap.20141219.122106
Creation date: Dec 19 12:21:06 2014
Junos version: 15.1-20141216_ib_15_1_psd.0
```

show system snapshot media

Syntax	<code>show system snapshot media <i>media-type</i></code>
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Display the snapshot information for both root partitions on SRX Series devices
Options	<ul style="list-style-type: none"> • <code>internal</code>— Show snapshot information from internal media. • <code>usb</code>— Show snapshot information from device connected to USB port. • <code>external</code>— Show snapshot information from the external CompactFlash card.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166
List of Sample Output	show system snapshot media internal on page 414 show system snapshot media usb on page 414

Sample Output

show system snapshot media internal

```
show system snapshot media internal
Information for snapshot on      internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos   : 10.1B3-domestic
Information for snapshot on      internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos   : 10.2-20100112.0-domestic
```

show system snapshot media usb

```
show system snapshot media usb
Information for snapshot on      usb (/dev/dals1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/dals2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```

show system storage partitions (EX Series Switches Only)

Syntax	show system storage partitions <all-members> <local> <member <i>member-id</i> >
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Display information about the disk partitions on EX Series switches.
Options	<p>none—Display partition information.</p> <p>all-members—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.</p> <p>local—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.</p> <p>member <i>member-id</i>—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 131
List of Sample Output	show system storage partitions on page 416
Output Fields	Table 55 describes the output fields for the show system storage partitions command. Output fields are listed in the approximate order in which they appear.

Table 55: show system storage partitions Output Fields

Field Name	Field Description
Boot Media	Media (internal or external) from which the switch was booted.
Active Partition	Name of the active root partition.
Backup Partition	Name of the backup (alternate) root partition.
Currently booted from	Partition from which the switch was last booted.
Partitions information	Information about partitions on the boot media: <ul style="list-style-type: none"> • Partition—Partition identifier. • Size—Size of partition. • Mountpoint—Directory on which the partition is mounted.

Sample Output

show system storage partitions

```
user@switch> show system storage partitions
fpc0:
-----
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:
  Partition  Size  Mountpoint
  s1a        184M  /
  s2a        184M  altroot
  s3d        369M  /var/tmp
  s3e        123M  /var
  s4d         62M  /config
  s4e                unused (backup config)
```


show system storage partitions (View SRX Series)

Syntax	show system storage partitions
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Display the partitioning scheme details on SRX Series devices.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	show system storage partitions (single root partitioning) on page 417 show system storage partitions (USB) on page 417

show system storage partitions (dual root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)
```

```
Partitions Information:
Partition Size Mountpoint
s1a 293M altroot
s2a 293M /
s3e 24M /config
s3f 342M /var
s4a 30M recovery
```

show system storage partitions (single root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Partitions Information:
Partition Size Mountpoint
s1a 898M /
s1e 24M /config
s1f 61M /var
```

show system storage partitions (USB)

```
show system storage partitions
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)
```

```
Partitions Information:
Partition Size Mountpoint
s1a 293M /
s2a 293M altroot
s3e 24M /config
```

s3f	342M	/var
s4a	30M	recovery

CLI User Guide

CHAPTER 19

Overview

- [Introducing the Junos OS Command-Line Interface on page 421](#)
- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 423](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 426](#)
- [Commands and Configuration Statements for Junos-FIPS on page 426](#)

Introducing the Junos OS Command-Line Interface

The Junos[®] operating system (Junos OS) command-line interface (CLI) is the software interface you use to access a device running Junos OS—whether from the console or through a network connection.

The Junos OS CLI is a Juniper Networks-specific command shell that runs on top of a FreeBSD UNIX-based operating system kernel. By leveraging industry-standard tools and utilities, the CLI provides a powerful set of commands that you can use to monitor and configure devices running Junos OS (see [Figure 10](#)).

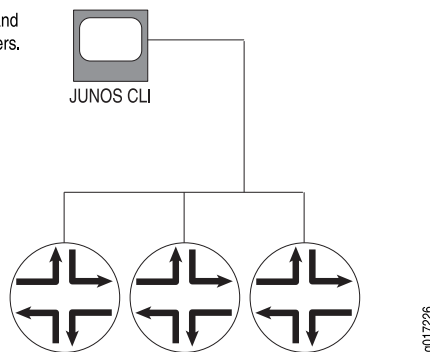
The Junos OS CLI has two modes:

- **Operational mode**—This mode displays the current status of the device. In operational mode, you enter commands to monitor and troubleshoot the Junos OS, devices, and network connectivity.
- **Configuration mode**—This mode enables you to configure the device. A configuration is stored as a hierarchy of configuration statements. In this mode, you enter statements to configure all properties of the device, including interfaces, general routing information, routing protocols, user access, and several system and hardware properties.

When you enter configuration mode, you are actually viewing and changing a file called the *candidate configuration*. The candidate configuration file enables you to make configuration changes without causing operational changes to the current operating configuration, called the *active configuration*. The router or switch does not implement the changes you added to the candidate configuration file until you commit them, which activates the configuration on the device. Candidate configurations enable you to alter your configuration without causing potential damage to your current network operations.

Figure 10: Monitoring and Configuring Routers

Use the JUNOS CLI to monitor and configure Juniper Networks routers.



Key Features of the CLI

The Junos OS CLI commands and statements follow a hierarchal organization and have a regular syntax. The Junos OS CLI provides the following features to simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software on which they are operating. For example, all **show** commands display software information and statistics, and all **clear** commands erase various types of system information.
- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command. This means that if you already are familiar with the Junos OS or with other routing software, you can use many of the CLI commands without referring to the documentation.
- Command completion—Command completion for command names (keywords) and for command options is available at each level of the hierarchy. To complete a command or option that you have partially typed, press the Tab key or the Spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command, and the possible completions are displayed. Completion also applies to other strings, such as filenames, interface names, usernames, and configuration statements.

If you have typed the mandatory arguments for executing a command in the operational or configuration mode the CLI displays **<[Enter]>** as one of the choices when you type a question mark (?). This indicates that you have entered the mandatory arguments and can execute the command at that level without specifying any further options. Likewise, the CLI also displays **<[Enter]>** when you have reached a specific hierarchy level in the configuration mode and do not have to enter any more mandatory arguments or statements.

- Industry-standard technology—With FreeBSD UNIX as the kernel, a variety of UNIX utilities are available on the Junos OS CLI. For example, you can:
 - Use regular expression matching to locate and replace values and identifiers in a configuration, filter command output, or examine log file entries.

- Use Emacs-based key sequences to move around on a command line and scroll through the recently executed commands and command output.
- Store and archive Junos OS device files on a UNIX-based file system.
 - Use standard UNIX conventions to specify filenames and paths.
- Exit from the CLI environment and create a UNIX C shell or Bourne shell to navigate the file system, manage router processes, and so on.

Related Documentation

- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 423](#)
- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 426](#)
- [Commands and Configuration Statements for Junos-FIPS on page 426](#)

Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies

The Junos OS command-line interface (CLI) commands and statements are organized under two command modes and various hierarchies. The following sections provide you an overview of the Junos OS CLI command modes and commands and statements hierarchies:

- [Junos OS CLI Command Modes on page 423](#)
- [CLI Command Hierarchy on page 424](#)
- [Configuration Statement Hierarchy on page 424](#)
- [Moving Among Hierarchy Levels on page 425](#)

Junos OS CLI Command Modes

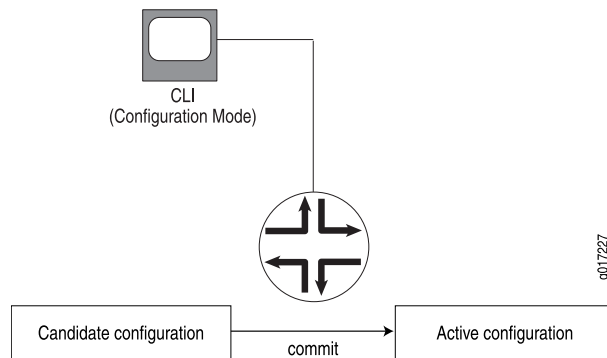
The Junos OS CLI has two modes:

- **Operational mode**—This mode displays the current status of the device. In operational mode, you enter commands to monitor and troubleshoot the Junos OS, devices, and network connectivity.
- **Configuration mode**—A configuration for a device running on Junos OS is stored as a hierarchy of statements. In configuration mode, you enter these statements to define all properties of the Junos OS, including interfaces, general routing information, routing protocols, user access, and several system and hardware properties.

When you enter configuration mode, you are actually viewing and changing a file called the *candidate configuration*. The candidate configuration file enables you to make configuration changes without causing operational changes to the current operating configuration, called the *active configuration*. The router or switch does not implement the changes you added to the candidate configuration file until you commit them, which activates the configuration on the router or switch (see [Figure 11](#)). Candidate configurations

enable you to alter your configuration without causing potential damage to your current network operations.

Figure 11: Committing a Configuration



CLI Command Hierarchy

CLI commands are organized in a hierarchy. Commands that perform a similar function are grouped together under the same level of the hierarchy. For example, all commands that display information about the system and the system software are grouped under the **show system** command, and all commands that display information about the routing table are grouped under the **show route** command.

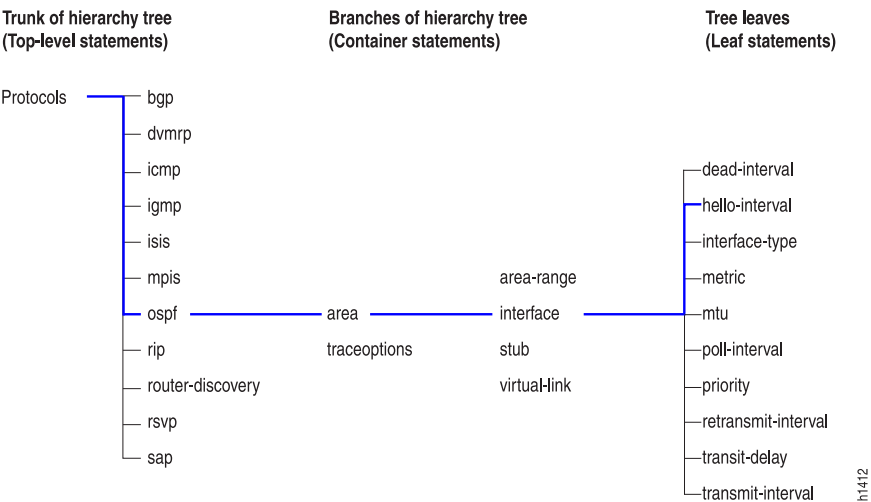
To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of the routes in the routing table, use the command **show route brief**.

Configuration Statement Hierarchy

The configuration statement hierarchy has two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not contain other statements. All of the container and leaf statements together form the *configuration hierarchy*.

Figure 12 illustrates a part of the hierarchy tree. The **protocols** statement is a top-level statement at the trunk of the configuration tree. The **ospf**, **area**, and **interface** statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree), and the **hello-interval** statement is a leaf on the tree.

Figure 12: Configuration Statement Hierarchy Example



Moving Among Hierarchy Levels

You can use the CLI commands in Table 56 to navigate the levels of the configuration statement hierarchy.

Table 56: CLI Configuration Mode Navigation Commands

Command	Description
edit <i>hierarchy-level</i>	Moves to an existing configuration statement hierarchy or creates a hierarchy and moves to that level.
exit	Moves up the hierarchy to the previous level where you were working. This command is, in effect, the opposite of the edit command. Alternatively, you can use the quit command. The exit and quit commands are interchangeable.
up	Moves up the hierarchy one level at a time.
top	Moves directly to the top level of the hierarchy.

Related Documentation

- [Introducing the Junos OS Command-Line Interface on page 421](#)
- [Getting Started with the Junos OS Command-Line Interface on page 429](#)

Other Tools to Configure and Monitor Devices Running Junos OS

Apart from the command-line interface, Junos OS also supports the following applications, scripts, and utilities that enable you to configure and monitor devices running Junos OS:

- J-Web graphical user interface (GUI)—Allows you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled. For more information, see the *J-Web Interface User Guide*.
- Junos XML management protocol—Application programmers can use the Junos XML management protocol to monitor and configure Juniper Networks routers. Juniper Networks provides a Perl module with the API to help you more quickly and easily develop custom Perl scripts for configuring and monitoring routers. For more information, see the *Junos XML Management Protocol Developer Guide*.
- NETCONF Application Programming Interface (API)—Application programmers can also use the NETCONF XML management protocol to monitor and configure Juniper Networks routers. For more information, see the *NETCONF XML Management Protocol Developer Guide*.
- Junos OS commit scripts and self-diagnosis features—You can define scripts to enforce custom configuration rules, use commit script macros to provide simplified aliases for frequently used configuration statements, and configure diagnostic event policies and actions associated with each policy. For more information, see the *Automation Scripting Feature Guide*.
- Management Information Bases (MIBs)—You can use enterprise-specific and standard MIBs to retrieve information about the hardware and software components on a Juniper Networks router. For more information about MIBs, see the *Network Management Administration Guide for Routing Devices*.

Related Documentation

- [Introducing the Junos OS Command-Line Interface on page 421](#)
- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
- [Commands and Configuration Statements for Junos-FIPS on page 426](#)

Commands and Configuration Statements for Junos-FIPS

Junos-FIPS enables you to configure a network of Juniper Networks routers in a Federal Information Processing Standards (FIPS) 140-2 environment.

The Junos-FIPS software environment requires the installation of FIPS software by a crypto officer. In Junos-FIPS, some Junos OS commands and statements have restrictions and some additional configuration statements are available. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

Related Documentation

- *Junos Secure Configuration Guide for Common Criteria and Junos-FIPS*
- *IPsec System Requirements for Junos-FIPS*

- *Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode*

Getting Started: A Quick Tour of the CLI

- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 431](#)
- [Configuring a User Account on a Device Running Junos OS on page 432](#)
- [Using the CLI Editor in Configuration Mode on page 434](#)
- [Checking the Status of a Device Running Junos OS on page 436](#)
- [Example: Configuring a Routing Protocol on page 438](#)
- [Rolling Back Junos OS Configuration Changes on page 444](#)

Getting Started with the Junos OS Command-Line Interface

As an introduction to the Junos OS command-line interface (CLI), this topic provides instructions for simple steps you take after installing Junos OS on the device. It shows you how to start the CLI, view the command hierarchy, and make small configuration changes. The related topics listed at the end of this topic provide you more detailed information about using the CLI.



NOTE:

- The instructions and examples in this topic are based on sample M Series and T Series routers. You can use them as a guideline for entering commands on your devices running Junos OS.
- Before you begin, make sure your device hardware is set up and Junos OS is installed. You must have a direct console connection to the device or network access using SSH or Telnet. If your device is not set up, follow the installation instructions provided with the device before proceeding.

To log in to a router and start the CLI:

1. Log in as **root**.

The root login account has superuser privileges, with access to all commands and statements.

2. Start the CLI:

```
root# cli
```

```
root@>
```

The > command prompt shows you are in operational mode. Later, when you enter configuration mode, the prompt will change to #.



NOTE: If you are using the root account for the first time on the device, remember that the device ships with no password required for root, but the first time you commit a configuration with Junos OS Release 7.6 or later, you must set a root password. Root access is not allowed over a telnet session. To enable root access over an SSH connection, you must configure the `system services ssh root-login allow` statement.

The CLI includes several ways to get help about commands. This section shows some examples of how to get help:

1. Type `?` to show the top-level commands available in operational mode.

```
root@> ?
Possible completions:
clear          Clear information in the system
configure      Manipulate software configuration information
diagnose       Invoke diagnose script
file           Perform file operations
help           Provide help information
monitor        Show real-time debugging information
mtrace         Trace multicast path from source to receiver
ping           Ping remote target
quit           Exit the management session
request        Make system-level requests
restart        Restart software process
set            Set CLI properties, date/time, craft interface message
show           Show system information
ssh            Start secure shell on another host
start          Start shell
telnet         Telnet to another host
test           Perform diagnostic debugging
traceroute     Trace route to remote host
```

2. Type `file ?` to show all possible completions for the `file` command.

```
root@> file ?
Possible completions:
<[Enter]>      Execute this command
archive        Archives files from the system
checksum       Calculate file checksum
compare        Compare files
copy           Copy files (local or remote)
delete         Delete files from the system
list           List file information
rename         Rename files
show           Show file contents
source-address Local address to use in originating the connection
|             Pipe through a command
```

3. Type `file archive ?` to show all possible completions for the `file archive` command.

```
root@> file archive ?
```

Possible completions:

compress	Compresses the archived file using GNU gzip (.tgz)
destination	Name of created archive (URL, local, remote, or floppy)
source	Path of directory to archive

Related Documentation

- [Getting Online Help from the Junos OS Command-Line Interface on page 447](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 431](#)
- [Checking the Status of a Device Running Junos OS on page 436](#)
- [Configuring a User Account on a Device Running Junos OS on page 432](#)
- [Configuring a Routing Protocol on page 438](#)
- [Examples: Using the Junos OS CLI Command Completion on page 453](#)

Switching Between Junos OS CLI Operational and Configuration Modes

When you monitor and configure a device running Junos OS, you may need to switch between operational mode and configuration mode. When you change to configuration mode, the command prompt also changes. The operational mode prompt is a right angle bracket (>) and the configuration mode prompt is a pound sign (#).

To switch between operational mode and configuration mode:

1. When you log in to the router and type the **cli** command, you are automatically in operational mode:

```
--- JUNOS 9.2B1.8 built 2008-05-09 23:41:29 UTC
% cli
user@host>
```

2. To enter configuration mode, type the **configure** command or the **edit** command from the CLI operation mode. For example:

```
user@host> configure
Entering configuration mode
```

```
[edit]
user@host#
```

The CLI prompt changes from **user@host>** to **user@host#** and a banner appears to indicate the hierarchy level.

3. You can return to operational mode in one of the following ways:

- To commit the configuration and exit:

```
[edit]
user@host# commit and-quit
commit complete
Exiting configuration mode
user@host>
```

- To exit without committing:

```
[edit]
```

```
user@host# exit
Exiting configuration mode
user@host>
```

When you exit configuration mode, the CLI prompt changes from **user@host#** to **user@host>** and the banner no longer appears. You can enter or exit configuration mode as many times as you wish without committing your changes.

4. To display the output of an operational mode command, such as **show**, while in configuration mode, issue the **run** configuration mode command and then specify the operational mode command:

```
[edit]
user@host# run operational-mode-command
```

For example, to display the currently set priority value of the Virtual Router Redundancy Protocol (VRRP) primary router while you are modifying the VRRP configuration for a backup router:

```
[edit interfaces xe-4/2/0 unit 0 family inet vrrp-group 27]
user@host# show
virtual-address [ 192.168.1.15 ];
[edit interfaces xe-4/2/0 unit 0 family inet vrrp-group 27]
user@host# run show vrrp detail
Physical interface: xe-5/2/0, Unit: 0, Address: 192.168.29.10/24
Interface state: up, Group: 10, State: backup
Priority: 190, Advertisement interval: 3, Authentication type: simple
Preempt: yes, VIP count: 1, VIP: 192.168.29.55
Dead timer: 8.326, Master priority: 201, Master router: 192.168.29.254
[edit interfaces xe-4/2/0 unit 0 family inet vrrp-group 27]
user@host# set priority ...
```

Related Documentation

- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 423](#)
- [Getting Online Help from the Junos OS Command-Line Interface on page 447](#)
- [Configuring a User Account on a Device Running Junos OS on page 432](#)

Configuring a User Account on a Device Running Junos OS

This topic describes how to log on to a device running Junos OS using a root account and configure a new user account. You can configure an account for your own use or create a test account.

To configure a new user account on the device:

1. Log in as root and enter configuration mode:

```
root@host> configure
[edit]
root@host#
```

The prompt in brackets (**[edit]**), also known as a *banner*, shows that you are in configuration edit mode at the top of the hierarchy.

2. Change to the **[edit system login]** section of the configuration:

```
[edit]
root@host# edit system login
[edit system login]
root@host#
```

The prompt in brackets changes to **[edit system login]** to show that you are at a new level in the hierarchy.

3. Now add a new user account:

```
[edit system login]
root@host# edit user nchen
```

This example adds an account **nchen** (for Nathan Chen).



NOTE: In Junos OS Release 12.2 and later, user account names can contain a period (.) in the name. For example, you can have a user account named **nathan.chen**. However, the username cannot begin or end with a period.

4. Configure a full name for the account. If the name includes spaces, enclose the entire name in quotation marks (" "):

```
[edit system login user nchen]
root@host# set full-name "Nathan Chen"
```

5. Configure an account class. The account class sets the user access privileges for the account:

```
[edit system login user nchen]
root@host# set class super-user
```

6. Configure an authentication method and password for the account:

```
[edit system login user nchen]
root@host# set authentication plain-text-password
New password:
Retype new password:
```

When the new password prompt appears, enter a clear-text password that the system can encrypt, and then confirm the new password.

7. Commit the configuration:

```
[edit system login user nchen]
root@host# commit
commit complete
```

Configuration changes are not activated until you commit the configuration. If the commit is successful, a **commit complete** message appears.

8. Return to the top level of the configuration, and then exit:

```
[edit system login user nchen]
root@host# top
[edit]
root@host# exit
Exiting configuration mode
```

9. Log out of the device:

```
root@host> exit
% logout Connection closed.
```

10. To test your changes, log back in with the user account and password you just configured:

```
login: nchen
Password: password
--- Junos 8.3-R1.1 built 2005-12-15 22:42:19 UTC
nchen@host>
```

When you log in, you should see the new username at the command prompt.

You have successfully used the CLI to view the device status and perform a simple configuration change. See the related topics listed in this section for more information about the Junos OS CLI features.



NOTE: For complete information about the commands to issue to configure your device, including examples, see the Junos OS configuration guides.

Related Documentation

- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
- [Getting Online Help from the Junos OS Command-Line Interface on page 447](#)
- [Displaying the Junos OS CLI Command and Word History on page 454](#)
- [Configuring a Routing Protocol on page 438](#)

Using the CLI Editor in Configuration Mode

This topic describes some of the basic commands that you must use to enter configuration mode in the command-line interface (CLI) editor, navigate through the configuration hierarchy, get help, and commit or revert the changes that you make during the configuration session.

Task	Command/Statement	Example
Edit Your Configuration		
Enter configuration mode.	configure	user@host> configure
When you first log in to the device, the device is in operational mode. You must explicitly enter configuration mode. When you do, the CLI prompt changes from user@host> to user@host# and the hierarchy level appears in square brackets.		[edit] user@host#

Task	Command/Statement	Example
<p>Create a statement hierarchy.</p> <p>You can use the edit command to simultaneously create a hierarchy and move to that new level in the hierarchy. You cannot use the edit command to change the value of identifiers.</p>	edit <i>hierarchy-level value</i>	<pre>[edit] user@host# edit security zones security-zone myzone [edit security zones security-zone myzone] user@host#</pre>
<p>Create a statement hierarchy and set identifier values.</p> <p>The set command is similar to edit except that your current level in the hierarchy does not change.</p>	set <i>hierarchy-level value</i>	<pre>[edit] user@host# set security zones security-zone myzone [edit] user@host#</pre>
Navigate the Hierarchy		
Navigate down to an existing hierarchy level.	edit <i>hierarchy-level</i>	<pre>[edit] user@host# edit security zones [edit security zones] user@host#</pre>
Navigate up one level in the hierarchy.	up	<pre>[edit security zones] user@host# up [edit security] user@host#</pre>
Navigate to the top of the hierarchy.	top	<pre>[edit security zones] user@host# top [edit] user@host#</pre>
Commit or Revert Changes		
Commit your configuration.	commit	<pre>[edit] user@host# commit commit complete</pre>
<p>Roll back changes from the current session.</p> <p>Use the rollback command to revert all changes from the current configuration session. When you run the rollback command before exiting your session or committing changes, the software loads the most recently committed configuration onto the device. You must enter the rollback statement at the edit level in the hierarchy.</p>	rollback	<pre>[edit] user@host# rollback load complete</pre>
Exit Configuration Mode		

Task	Command/Statement	Example
Commit the configuration and exit configuration mode.	commit and-quit	[edit] user@host# commit and-quit user@host>
Exit configuration mode without committing your configuration. You must navigate to the top of the hierarchy using the up or top commands before you can exit configuration mode.	exit	[edit] user@host# exit The configuration has been changed but not committed Exit with uncommitted changes? [yes,no] (yes)
Get Help		
Display a list of valid options for the current hierarchy level.	?	[edit] user@host# edit security zones ? Possible completions: <[Enter]> Execute this command > functional-zone Functional zone > security-zone Security zones Pipe through a command [edit]

- Related Documentation**
- [Understanding Junos OS CLI Configuration Mode on page 456](#)
 - [Entering and Exiting the Junos OS CLI Configuration Mode on page 462](#)
 - [Displaying the Current Junos OS Configuration on page 497](#)

Checking the Status of a Device Running Junos OS

You can use **show** commands to check the status of the device and monitor the activities on the device.

To help you become familiar with **show** commands:

- Type **show ?** to display the list of **show** commands you can use to monitor the router:

```
root@> show ?
Possible completions:
accounting      Show accounting profiles and records
aps             Show Automatic Protection Switching information
arp            Show system Address Resolution Protocol table entries
as-path        Show table of known autonomous system paths
bfd            Show Bidirectional Forwarding Detection information
bgp            Show Border Gateway Protocol information
chassis        Show chassis information
class-of-service Show class-of-service (CoS) information
cli            Show command-line interface settings
configuration   Show current configuration
connections     Show circuit cross-connect connections
dvmrp          Show Distance Vector Multicast Routing Protocol
info
dynamic-tunnels Show dynamic tunnel information information
esis           Show end system-to-intermediate system information
```

firewall	Show firewall information
helper	Show port-forwarding helper information
host	Show hostname information from domain name server
igmp	Show Internet Group Management Protocol information
ike	Show Internet Key Exchange information
ilmi	Show interim local management interface information
interfaces	Show interface information
ipsec	Show IP Security information
ipv6	Show IP version 6 information
isis	Show Intermediate System-to-Intermediate System info
l2circuit	Show Layer 2 circuit information
l2vpn	Show Layer 2 VPN information
lacp	Show Link Aggregation Control Protocol information
ldp	Show Label Distribution Protocol information
link-management	Show link management information
llc2	Show LLC2 protocol related information
log	Show contents of log file
mld	Show multicast listener discovery information
mpls	Show Multiprotocol Label Switching information
msdp	Show Multicast Source Discovery Protocol information
multicast	Show multicast information
ntp	Show Network Time Protocol information
ospf	Show Open Shortest Path First information
ospf3	Show Open Shortest Path First version 3 information
passive-monitoring	Show information about passive monitoring
pfe	Show Packet Forwarding Engine information
pgm	Show Pragmatic Generalized Multicast information
pim	Show Protocol Independent Multicast information
policer	Show interface policer counters and information
policy	Show policy information
ppp	Show PPP process information
rip	Show Routing Information Protocol information
ripng	Show Routing Information Protocol for IPv6 info
route	Show routing table information
rsvp	Show Resource Reservation Protocol information
sap	Show Session Announcement Protocol information
security	Show security information
services	Show services information
snmp	Show Simple Network Management Protocol information
system	Show system information
task	Show routing protocol per-task information
ted	Show Traffic Engineering Database information
version	Show software process revision levels
vpls	Show VPLS information
vrrp	Show Virtual Router Redundancy Protocol information

- Use the **show chassis routing-engine** command to view the Routing Engine status:

```

root@> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state           Master
  Election priority       Master (default)
  Temperature             31 degrees C / 87 degrees F
  CPU temperature         32 degrees C / 89 degrees F
  DRAM                    768 MB
  Memory utilization      84 percent
  CPU utilization:
    User                  0 percent
    Background            0 percent
    Kernel                1 percent
    Interrupt             0 percent

```

```

Idle 99 percent
Model RE-2.0
Serial ID b10000078c10d701
Start time 2005-12-28 13:52:00 PST
Uptime 12 days, 3 hours, 44 minutes, 19 seconds
Load averages: 1 minute 5 minute 15 minute
                 0.02      0.01      0.00

```

- Use the **show system storage** command to view available storage on the device:

```
root@> show system storage
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s1a	865M	127M	669M	16%	/
devfs	1.0K	1.0K	0B	100%	/dev
devfs	1.0K	1.0K	0B	100%	/dev/
/dev/md0	30M	30M	0B	100%	/packages/mnt/jbase
/dev/md1	158M	158M	0B	100%	
/packages/mnt/jkernel-9.3B1.5					
/dev/md2	16M	16M	0B	100%	
/packages/mnt/jpfe-M7i-9.3B1.5					
/dev/md3	3.8M	3.8M	0B	100%	
/packages/mnt/jdocs-9.3B1.5					
/dev/md4	44M	44M	0B	100%	
/packages/mnt/jroute-9.3B1.5					
/dev/md5	12M	12M	0B	100%	
/packages/mnt/jcrypto-9.3B1.5					
/dev/md6	25M	25M	0B	100%	
/packages/mnt/jpfe-common-9.3B1.5					
/dev/md7	1.5G	196K	1.4G	0%	/tmp
/dev/md8	1.5G	910K	1.4G	0%	/mfs
/dev/ad0s1e	96M	38K	88M	0%	/config
procfs	4.0K	4.0K	0B	100%	/proc
/dev/ad1s1f	17G	2.6G	13G	17%	/var

Related Documentation

- [Displaying the Junos OS CLI Command and Word History on page 454](#)
- [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 579](#)
- [Viewing Files and Directories on a Device Running Junos OS on page 573](#)

Example: Configuring a Routing Protocol

This topic provides a sample configuration that describes how to configure an OSPF backbone area that has two SONET interfaces.

The final configuration looks like this:

```

[edit]
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {

```

```

        hello-interval 5;
        dead-interval 20;
    }
}
}
}

```

This topic contains the following examples of configuring a routing protocol:

- [Shortcut on page 439](#)
- [Longer Configuration on page 439](#)
- [Making Changes to a Routing Protocol Configuration on page 441](#)

Shortcut

You can create a shortcut for this entire configuration with the following two commands:

```

[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
               dead-interval 20
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/1 hello-interval 5
               dead-interval 20

```

Longer Configuration

This section provides a longer example of creating the previous OSPF configuration. In the process, it illustrates how to use the different features of the CLI.

1. Enter configuration mode by issuing the **configure** top-level command:

```

user@host> configure
entering configuration mode
[edit]
user@host#

```

Notice that the prompt has changed to a pound sign (#) to indicate configuration mode.

2. To create the above configuration, you start by editing the **protocols ospf** statements:

```

[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host#

```

3. Now add the OSPF area:

```

[edit protocols ospf]
user@host# edit area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host#

```

4. Add the first interface:

```

[edit protocols ospf area 0.0.0.0]
user@host# edit interface so0
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]

```

```
user@host#
```

You now have four nested statements.

5. Set the hello and dead intervals.

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# set ?
user@host# set hello-interval 5
user@host# set dead-interval 20
user@host#
```

6. You can see what is configured at the current level with the **show** command:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# show
hello-interval 5;
dead-interval 20;
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host#
```

7. You are finished at this level, so back up a level and take a look at what you have so far:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# up
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
    hello-interval 5;
    dead-interval 20;
}
[edit protocols ospf area 0.0.0.0]
user@host#
```

The **interface** statement appears because you have moved to the **area** statement.

8. Add the second interface:

```
[edit protocols ospf area 0.0.0.0]
user@host# edit interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set hello-interval 5
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set dead-interval 20
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# up
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
    hello-interval 5;
    dead-interval 20;
}
interface so-0/0/1 {
    hello-interval 5;
    dead-interval 20;
}
[edit protocols ospf area 0.0.0.0]
user@host#
```


9. Back up to the top level and see what you have:

```
[edit protocols ospf area 0.0.0.0]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
      }
    }
  }
}
[edit]
user@host#
```

This configuration now contains the statements you want.

10. Before committing the configuration (and thereby activating it), verify that the configuration is correct:

```
[edit]
user@host# commit check
configuration check succeeds
[edit]
user@host#
```

11. Commit the configuration to activate it on the router:

```
[edit]
user@host# commit
commit complete
[edit]
user@host#
```

Making Changes to a Routing Protocol Configuration

Suppose you decide to use different dead and hello intervals on interface **so-0/0/1**. You can make changes to the configuration.

1. Go directly to the appropriate hierarchy level by typing the full hierarchy path to the statement you want to edit:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# show
hello-interval 5;
dead-interval 20;
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
```

```

user@host# set hello-interval 7
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set dead-interval 28
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
        dead-interval 20;
      }
      interface so-0/0/1 {
        hello-interval 7;
        dead-interval 28;
      }
    }
  }
}
[edit]
user@host#

```

2. If you decide not to run OSPF on the first interface, delete the statement:

```

[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# delete interface so-0/0/0
[edit protocols ospf area 0.0.0.0]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1 {
        hello-interval 7;
        dead-interval 28;
      }
    }
  }
}
[edit]
user@host#

```

Everything inside the statement you deleted was deleted with it. You can also eliminate the entire OSPF configuration by simply entering **delete protocols ospf** while at the top level.

3. If you decide to use the default values for the hello and dead intervals on your remaining interface but you want OSPF to run on that interface, delete the hello and dead interval timers:

```

[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1

```

```

[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# delete hello-interval
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# delete dead-interval
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# top
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1;
    }
  }
}
[edit]
user@host#

```

You can set multiple statements at the same time as long as they are all part of the same hierarchy (the path of statements from the top inward, as well as one or more statements at the bottom of the hierarchy). This feature can reduce considerably the number of commands you must enter.

4. To go back to the original hello and dead interval timers on interface **so-0/0/1**, enter:

```

[edit]
user@host# edit protocols ospf area 0.0.0.0 interface so-0/0/1
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# set hello-interval 5 dead-interval 20
[edit protocols ospf area 0.0.0.0 interface so-0/0/1]
user@host# exit
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
      }
    }
  }
}
[edit]
user@host#

```

5. You also can recreate the other interface, as you had it before, with only a single entry:

```

[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/1 hello-interval 5
dead-interval 20
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {

```

```
        hello-interval 5;
        dead-interval 20;
    }
    interface so-0/0/1 {
        hello-interval 5;
        dead-interval 20;
    }
}
}
[edit]
user@host#
```

- Related Documentation**
- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
 - [Displaying the Junos OS CLI Command and Word History on page 454](#)
 - [Interface Naming Conventions Used in the Junos OS Operational Commands on page 572](#)

Rolling Back Junos OS Configuration Changes

This topic shows how to use the **rollback** command to return to the most recently committed Junos OS configuration. The **rollback** command is useful if you make configuration changes and then decide not to keep the changes.

The following procedure shows how to configure an SNMP health monitor on a device running Junos OS and then return to the most recently committed configuration that does not include the health monitor. When configured, the SNMP health monitor provides the network management system (NMS) with predefined monitoring for file system usage, CPU usage, and memory usage on the device.

1. Enter configuration mode:

```
user@host> configure
entering configuration mode
[edit]
user@host#
```

2. Show the current configuration (if any) for SNMP:

```
[edit]
user@host# show snmp
```

No **snmp** statements appear because SNMP has not been configured on the device.

3. Configure the health monitor:

```
[edit]
user@host# set snmp health-monitor
```

4. Show the new configuration:

```
[edit]
user@host# show snmp
health-monitor;
```

The **health-monitor** statement indicates that SNMP health monitoring is configured on the device.

5. Enter the **rollback** configuration mode command to return to the most recently committed configuration:

```
[edit]
user@host# rollback
load complete
```

6. Show the configuration again to make sure your change is no longer present:

```
[edit]
user@host# show snmp
```

No **snmp** configuration statements appear. The health monitor is no longer configured.

7. Enter the **commit** command to activate the configuration to which you rolled back:

```
[edit]
user@host# commit
```

8. Exit configuration mode:

```
[edit]
user@host# exit
Exiting configuration mode
```

You can also use the **rollback** command to return to earlier configurations.

Related Documentation

- [Returning to the Most Recently Committed Junos OS Configuration on page 534](#)

CHAPTER 21

Getting Online Help

- [Getting Online Help from the Junos OS Command-Line Interface on page 447](#)
- [Junos OS CLI Online Help Features on page 450](#)
- [Examples: Using Command Completion in Configuration Mode on page 451](#)
- [Examples: Using the Junos OS CLI Command Completion on page 453](#)
- [Displaying the Junos OS CLI Command and Word History on page 454](#)

Getting Online Help from the Junos OS Command-Line Interface

The Junos OS command-line interface (CLI) has a context-sensitive online help feature that enables you to access information about commands and statements from the Junos OS CLI. This topic contains the following sections:

- [Getting Help About Commands on page 447](#)
- [Getting Help About a String in a Statement or Command on page 448](#)
- [Getting Help About Configuration Statements on page 449](#)
- [Getting Help About System Log Messages on page 449](#)

Getting Help About Commands

Information about commands is provided at each level of the CLI command hierarchy. You can type a question mark to get help about commands:

- If you type the question mark at the command-line prompt, the CLI lists the available commands and options. For example, to view a list of top-level operational mode commands, type a question mark (?) at the command-line prompt.

```
user@host> ?
Possible completions:
clear          Clear information in the system
configure      Manipulate software configuration information
file           Perform file operations
help           Provide help information
mtrace         Trace mtrace packets from source to receiver.
monitor        Real-time debugging
ping           Ping a remote target
quit           Exit the management session
request        Make system-level requests
restart        Restart a software process
set            Set CLI properties, date, time, craft display text
```

```
show      Show information about the system
ssh       Open a secure shell to another host
start     Start a software process
telnet    Telnet to another host
test      Diagnostic debugging commands
traceroute Trace the route to a remote host
user@host>
```

- If you type the question mark after entering the complete name of a command or command option, the CLI lists the available commands and options and then redisplay the command names and options that you typed.

```
user@host> clear ?
Possible completions:
arp        Clear address-resolution information
bgp        Clear BGP information
chassis    Clear chassis information
firewall   Clear firewall counters
igmp       Clear IGMP information
interfaces Clear interface information
ilmi       Clear ILMI statistics information
isis       Clear IS-IS information
ldp        Clear LDP information
log        Clear contents of a log file
mpls       Clear MPLS information
msdp       Clear MSDP information
multicast  Clear Multicast information
ospf       Clear OSPF information
pim        Clear PIM information
rip        Clear RIP information
route      Clear routing table information
rsvp       Clear RSVP information
snmp       Clear SNMP information
system     Clear system status
vrrp       Clear VRRP statistics information
user@host> clear
```

- If you type the question mark in the middle of a command name, the CLI lists possible command completions that match the letters you have entered so far. It then redisplay the letters that you typed. For example, to list all operational mode commands that start with the letter *c*, type the following:

```
user@host> c?
Possible completions:
clear      Clear information in the system
configure  Manipulate software configuration information
user@host> c
```

- For introductory information on using the question mark or the help command, you can also type **help** and press Enter:

```
user@host> help
```

Getting Help About a String in a Statement or Command

You can use the **help** command to display help about a text string contained in a statement or command name:

```
help apropos string
```


string is a text string about which you want to get help. This string is used to match statement or command names as well as to match the help strings that are displayed for the statements or commands.

If the string contains spaces, enclose it in quotation marks (" "). You can also specify a regular expression for the string, using standard UNIX-style regular expression syntax.

For statements or commands which need input data type as STRING, the supported characters set are as follows:

- Any printable ASCII characters
- For characters with space, it should be enclosed in double-quotes
- To have double-quote as the input, it should be escaped with '\'



NOTE: No escape characters are supported in a string other than to escape from double quotes.

Range of supported characters for attributes is 0 through 65499 characters.

Range of supported characters for string type identifiers is 1 through 255 characters.

In configuration mode, this command displays statement names and help text that match the string specified. In operational mode, this command displays command names and help text that match the string specified.

Getting Help About Configuration Statements

You can display help based on text contained in a statement name using the **help topic** and **help reference** commands:

help topic *word*
help reference *statement-name*

The **help topic** command displays usage guidelines for the statement based on information that appears in the Junos OS configuration guides. The **help reference** command displays summary information about the statement based on the summary descriptions that appear in the Junos OS configuration guides.

Getting Help About System Log Messages

You can display help based on a system log tag using the **help syslog** command:

help syslog *syslog-tag*

The **help syslog** command displays the contents of a system log message.

Related Documentation

- [Junos OS CLI Online Help Features on page 450](#)
- [Getting Started with the Junos OS Command-Line Interface on page 429](#)

Junos OS CLI Online Help Features

The Junos OS CLI online help provides the following features for ease of use and error prevention:

- [Help for Omitted Statements on page 450](#)
- [Using CLI Command Completion on page 450](#)
- [Using Command Completion in Configuration Mode on page 451](#)
- [Displaying Tips About CLI Commands on page 451](#)

Help for Omitted Statements

If you have omitted a required statement at a particular hierarchy level, when you attempt to move from that hierarchy level or when you issue the **show** command in configuration mode, a message indicates which statement is missing. For example:

```
[edit protocols pim interface so-0/0/0]
user@host# top
Warning: missing mandatory statement: 'mode'
[edit]
user@host# show
protocols {
  pim {
    interface so-0/0/0 {
      priority 4;
      version 2;
      # Warning: missing mandatory statement(s): 'mode'
    }
  }
}
```

Using CLI Command Completion

The Junos OS CLI provides you a command completion option that enables Junos OS to recognize commands and options based on the initial few letters you typed. That is, you do not always have to remember or type the full command or option name for the CLI to recognize it.

- To display all possible command or option completions, type the partial command followed immediately by a question mark.
- To complete a command or option that you have partially typed, press Tab or the Spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a prompt indicates that you have entered an ambiguous command, and the possible completions are displayed.

Command completion also applies to other strings, such as filenames, interface names, and usernames. To display all possible values, type a partial string followed immediately by a question mark. To complete a string, press Tab.

Using Command Completion in Configuration Mode

The CLI command completion functions also apply to the commands in configuration mode and to configuration statements. Specifically, to display all possible commands or statements, type the partial string followed immediately by a question mark. To complete a command or statement that you have partially typed, press Tab or the Spacebar.

Command completion also applies to identifiers, with one slight difference. To display all possible identifiers, type a partial string followed immediately by a question mark. To complete an identifier, you must press Tab. This scheme allows you to enter identifiers with similar names; then press the Spacebar when you are done typing the identifier name.

Displaying Tips About CLI Commands

To get tips about CLI commands, issue the **help tip cli** command. Each time you enter the command, a new tip appears. For example:

```
user@host> help tip cli
Junos tip:
Use 'request system software validate' to validate the incoming software
against the current configuration without impacting the running system.
user@host> help tip cli
Junos tip:
Use 'commit and-quit' to exit configuration mode after the commit has
succeeded. If the commit fails, you are left in configuration mode.
```

You can also enter **help tip cli *number*** to associate a tip with a number. This enables you to recall the tip at a later time. For example:

```
user@host> help tip cli 10
JUNOS tip:
Use '#' in the beginning of a line in command scripts to cause the
rest of the line to be ignored.

user@host> help tip cli
JUNOS tip:
Use the 'apply-groups' statement at any level of the configuration
hierarchy to inherit configuration statements from a configuration group.

user@host>
```

Related Documentation

- [Getting Started with the Junos OS Command-Line Interface on page 429](#)
- [Examples: Using the Junos OS CLI Command Completion on page 453](#)

Examples: Using Command Completion in Configuration Mode

List the configuration mode commands:

```
[edit]
user@host# ?
  <[Enter]>      Execute this command
  activate      Remove the inactive tag from a statement
```

annotate	Annotate the statement with a comment
commit	Commit current set of changes
copy	Copy a statement
deactivate	Add the inactive tag to a statement
delete	Delete a data element
edit	Edit a sub-element
exit	Exit from this level
extension	Extension operations
help	Provide help information
insert	Insert a new ordered data element
load	Load configuration from ASCII file
quit	Quit from this level
rename	Rename a statement
replace	Replace character string in configuration
rollback	Roll back to previous committed configuration
run	Run an operational-mode command
save	Save configuration to ASCII file
set	Set a parameter
show	Show a parameter
status	Show users currently editing configuration
top	Exit to top level of configuration
up	Exit one level of configuration
wildcard	Wildcard operations

[edit]user@host#

List all the statements available at a particular hierarchy level:

```
[edit]
user@host# edit ?
Possible completions:
> accounting-options  Accounting data configuration
> chassis             Chassis configuration
> class-of-service    Class-of-service configuration
> firewall            Define a firewall configuration
> forwarding-options  Configure options to control packet sampling
> groups              Configuration groups
> interfaces          Interface configuration
> policy-options      Routing policy option configuration
> protocols            Routing protocol configuration
> routing-instances   Routing instance configuration
> routing-options      Protocol-independent routing option configuration
> snmp                Simple Network Management Protocol
> system              System parameters

user@host# edit protocols ?
Possible completions:
<[Enter]>             Execute this command
> bgp                 BGP options
> connections         Circuit cross-connect configuration
> dvmrp               DVMRP options
> igmp                IGMP options
> isis                IS-IS options
> ldp                 LDP options
> mpls                Multiprotocol Label Switching options
> msdp                MSDP options
> ospf                OSPF configuration
> pim                 PIM options
> rip                 RIP options
> router-discovery    ICMP router discovery options
> rsvp                RSVP options
> sapSession          Advertisement Protocol options
```

```

> vrrp                VRRP options
|                    Pipe through a command

[edit]
user@host# edit protocols
List all commands that start with a particular letter or string:

user@host# edit routing-options a?
Possible completions:
> aggregate           Coalesced routes
> autonomous-system   Autonomous system number

[edit]
user@host# edit routing-options a
List all configured Asynchronous Transfer Mode (ATM) interfaces:

[edit]
user@host# edit interfaces at?
<interface_name>      Interface name
  at-0/2/0             Interface name
  at-0/2/1             Interface name
[edit]
user@host# edit interfaces at

Display a list of all configured policy statements:

[edit]
user@host# show policy-options policy-statement ?
<policy_name>         Name to identify a policy filter
user@host# show policy-options policy-statement
  <policy_name>       Name to identify a policy filter
  lo0only-v4          Name to identify a policy filter
  lo0only-v6          Name to identify a policy filter
  lo2bgp              Name to identify a policy filter

```

- Related Documentation**
- [Examples: Using the Junos OS CLI Command Completion on page 453](#)
 - [Displaying the Junos OS CLI Command and Word History on page 454](#)

Examples: Using the Junos OS CLI Command Completion

The following examples show how you can use the command completion feature in Junos OS. Issue the **show interfaces** command:

```

user@host> sh<Space>ow i<Space>
'i' is ambiguous.
Possible completions:
igmp                Show information about IGMP
interface           Show interface information
isis                Show information about IS-IS

user@host> show in<Space>terfaces
Physical interface: at-0/1/0, Enabled, Physical link is Up
Interface index: 11, SNMP ifIndex: 65
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode
Speed: OC12, Loopback: None, Payload scrambler: Enabled
Device flags: Present Running
Link flags: 0x01
...

```

```
user@host>
```

Display a list of all log files whose names start with the string “messages,” and then display the contents of one of the files:

```
user@myhost> show log mes?
```

Possible completions:

```
<filename>Log file to display
messagesSize: 1417052, Last changed: Mar 3 00:33
messages.0.gzSize: 145575, Last changed: Mar 3 00:00
messages.1.gzSize: 134253, Last changed: Mar 2 23:00
messages.10.gzSize: 137022, Last changed: Mar 2 14:00
messages.2.grSize: 137112, Last changed: Mar 2 22:00
messages.3.gzSize: 121633, Last changed: Mar 2 21:00
messages.4.gzSize: 135715, Last changed: Mar 2 20:00
messages.5.gzSize: 137504, Last changed: Mar 2 19:00
messages.6.gzSize: 134591, Last changed: Mar 2 18:00
messages.7.gzSize: 132670, Last changed: Mar 2 17:00
messages.8.gzSize: 136596, Last changed: Mar 2 16:00
messages.9.gzSize: 136210, Last changed: Mar 2 15:00
```

```
user@myhost> show log mes<Tab>sages.4<Tab>.gz<Enter>
Jan 15 21:00:00 myhost newsyslog[1381]: logfile turned over
...
```

Related Documentation

- [Displaying the Junos OS CLI Command and Word History on page 454](#)

Displaying the Junos OS CLI Command and Word History

To display a list of recent commands that you issued, use the **show cli history** command:

```
user@host> show cli history 3
01:01:44 -- show bgp next-hop-database
01:01:51 -- show cli history
01:02:51 -- show cli history 3
```

You can press Esc+. (period) or Alt+. (period) to insert the last word of the previous command. Repeat Esc+. or Alt+. to scroll backwards through the list of recently entered words. For example:

```
user@host> show interfaces terse fe-0/0/0
Interface      Admin  Link  Proto  Local  Remote
fe-0/0/0        up     up    inet   192.168.220.1/30
fe-0/0/0.0      up     up    inet   192.168.220.1/30

user@host> <Esc>
user@host> fe-0/0/0
```

If you scroll completely to the beginning of the list, pressing Esc+. or Alt+. again restarts scrolling from the last word entered.

Related Documentation

- [Junos OS CLI Online Help Features on page 450](#)

CHAPTER 22

Using Configuration Statements to Configure a Device

- [Understanding Junos OS CLI Configuration Mode on page 456](#)
- [Entering and Exiting the Junos OS CLI Configuration Mode on page 462](#)
- [Notational Conventions Used in Junos OS Configuration Hierarchies on page 464](#)
- [Forms of the configure Command on page 465](#)
- [Using the configure exclusive Command on page 467](#)
- [Using the configure Command on page 468](#)
- [Modifying the Junos OS Configuration on page 468](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Deleting a Statement from a Junos OS Configuration on page 470](#)
- [Example: Deleting a Statement from the Junos OS Configuration on page 471](#)
- [Copying a Junos OS Statement in the Configuration on page 473](#)
- [Example: Copying a Statement in the Junos Configuration on page 473](#)
- [Issuing Relative Junos OS Configuration Mode Commands on page 475](#)
- [Renaming an Identifier in a Junos OS Configuration on page 476](#)
- [Examples: Re-Using Configuration on page 476](#)
- [Inserting a New Identifier in a Junos OS Configuration on page 481](#)
- [Example: Inserting a New Identifier in a Junos Configuration on page 481](#)
- [Example: Using the Wildcard Command with the Range Option on page 485](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489](#)
- [Example: Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 490](#)
- [Adding Comments in a Junos OS Configuration on page 492](#)
- [Example: Including Comments in a Junos OS Configuration by Using the CLI on page 494](#)
- [Updating the configure private Configuration on page 496](#)
- [Displaying the Current Junos OS Configuration on page 497](#)
- [Example: Displaying the Current Junos OS Configuration on page 498](#)

- [Displaying Additional Information About the Junos OS Configuration on page 499](#)
- [Displaying set Commands from the Junos OS Configuration on page 501](#)
- [Displaying Users Currently Editing the Junos OS Configuration on page 504](#)
- [Verifying a Junos OS Configuration on page 504](#)

[Understanding Junos OS CLI Configuration Mode](#)

You can configure all properties of Junos OS, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

As described in “[Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies](#)” on [page 423](#), a router configuration is stored as a hierarchy of statements. In configuration mode, you create the specific hierarchy of configuration statements that you want to use. When you have finished entering the configuration statements, you commit them, which activates the configuration on the router.

You can create the hierarchy interactively or you can create an ASCII text file that is loaded onto the router or switch and then committed.

This topic covers:

- [Configuration Mode Commands on page 457](#)
- [Configuration Statements and Identifiers on page 458](#)
- [Configuration Statement Hierarchy on page 460](#)

Configuration Mode Commands

Table 57 summarizes each CLI configuration mode command. The commands are organized alphabetically.

Table 57: Summary of Configuration Mode Commands

Command	Description
activate	Remove the inactive: tag from a statement, effectively reading the statement or identifier to the configuration. Statements or identifiers that have been activated take effect when you next issue the commit command.
annotate	Add comments to a configuration. You can add comments only at the current hierarchy level.
commit	Commit the set of changes to the database and cause the changes to take operational effect.
copy	Make a copy of an existing statement in the configuration.
deactivate	Add the inactive: tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the commit command.
delete	Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.
edit	Move inside the specified statement hierarchy. If the statement does not exist, it is created.
exit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.
extension	Manage configurations that are contributed by SDK application packages. Either display or delete user-defined configuration contributed by the named SDK application package. A configuration defined in any native Junos OS package is never deleted by the extension command.
help	Display help about available configuration statements.
insert	Insert an identifier into an existing hierarchy.
load	Load a configuration from an ASCII configuration file or from terminal input. Your current location in the configuration hierarchy is ignored when the load operation occurs.

Table 57: Summary of Configuration Mode Commands (*continued*)

Command	Description
quit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.
rename	Rename an existing configuration statement or identifier.
replace	Replace identifiers or values in a configuration.
rollback	Return to a previously committed configuration. The software saves the last 10 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command.
run	Run a top-level CLI command without exiting from configuration mode.
save	Save the configuration to an ASCII file. The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy.
set	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change.
show	Display the current configuration.
status	Display the users currently editing the configuration.
top	Return to the top level of configuration command mode, which is indicated by the [edit] banner.
up	Move up one level in the statement hierarchy.
update	Update a private database.
wildcard	Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it. You can use regular expressions to specify a pattern. Based on this pattern, you search for items that contain these patterns and delete them.

Configuration Statements and Identifiers

You can configure router or switch properties by including the corresponding statements in the configuration. Typically, a statement consists of a keyword, which is fixed text, and, optionally, an identifier. An identifier is an identifying name that you can define, such as

the name of an interface or a username, which enables you and the CLI to differentiate among a collection of statements.

Table 58 describes top-level CLI configuration mode statements.



NOTE: The QFX3500 switch does not support the IS-IS, OSPF, BGP, LDP, MPLS, and RSVP protocols.

Table 58: Configuration Mode Top-Level Statements

Statement	Description
access	Configure the Challenge Handshake Authentication Protocol (CHAP). For information about the statements in this hierarchy, see the <i>Junos OS Administration Library for Routing Devices</i> .
accounting-options	Configure accounting statistics data collection for interfaces and firewall filters. For information about the statements in this hierarchy, see the <i>Network Management Administration Guide for Routing Devices</i> .
chassis	Configure properties of the router chassis, including conditions that activate alarms and SONET/SDH framing and concatenation properties. For information about the statements in this hierarchy, see the <i>Junos OS Administration Library for Routing Devices</i> .
class-of-service	Configure class-of-service parameters. For information about the statements in this hierarchy, see the <i>Class of Service Feature Guide for Routing Devices</i> .
firewall	Define filters that select packets based on their contents. For information about the statements in this hierarchy, see the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i> .
forwarding-options	Define forwarding options, including traffic sampling options. For information about the statements in this hierarchy, see the <i>Junos OS Network Interfaces Library for Routing Devices</i> .
groups	Configure configuration groups. For information about statements in this hierarchy, see the <i>Junos OS Administration Library for Routing Devices</i> .
interfaces	Configure interface information, such as encapsulation, interfaces, virtual channel identifiers (VCIs), and data-link connection identifiers (DLCIs). For information about the statements in this hierarchy, see the <i>Junos OS Network Interfaces Library for Routing Devices</i> .
policy-options	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes. For information about the statements in this hierarchy, see the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i> .
protocols	Configure routing protocols, including BGP, IS-IS, LDP, MPLS, OSPF, RIP, and RSVP. For information about the statements in this hierarchy, see the chapters that discuss how to configure the individual routing protocols in the <i>Junos OS Routing Protocols Library for Routing Devices</i> and the <i>MPLS Applications Feature Guide for Routing Devices</i> .

Table 58: Configuration Mode Top-Level Statements (*continued*)

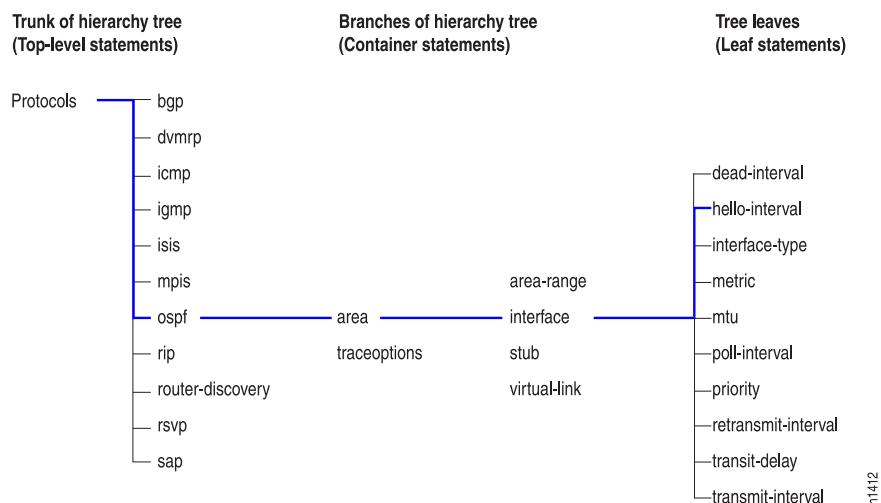
Statement	Description
routing-instances	Configure multiple routing instances. For information about the statements in this hierarchy, see the <i>Junos OS Routing Protocols Library for Routing Devices</i> .
routing-options	Configure protocol-independent routing options, such as static routes, autonomous system numbers, confederation members, and global tracing (debugging) operations to log. For information about the statements in this hierarchy, see the <i>Junos OS Routing Protocols Library for Routing Devices</i> .
security	Configure IP Security (IPsec) services. For information about the statements in this hierarchy see the <i>Junos OS Administration Library for Routing Devices</i> .
snmp	Configure SNMP community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the <i>Network Management Administration Guide for Routing Devices</i> .
system	Configure systemwide properties, including the hostname, domain name, Domain Name System (DNS) server, user logins and permissions, mappings between hostnames and addresses, and software processes. For information about the statements in this hierarchy, see the <i>Junos OS Administration Library for Routing Devices</i> .

For specific information on configuration statements, see the Junos OS configuration guides.

Configuration Statement Hierarchy

The Junos OS configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not contain other statements (see Figure 13). All of the container and leaf statements together form the *configuration hierarchy*.

Figure 13: Configuration Mode Hierarchy of Statements



Each statement at the top level of the configuration hierarchy resides at the trunk (or root level) of a hierarchy tree. The top-level statements are container statements, containing other statements that form the tree branches. The leaf statements are the leaves of the hierarchy tree. An individual hierarchy of statements, which starts at the trunk of the hierarchy tree, is called a *statement path*. [Figure 13](#) illustrates the hierarchy tree, showing a statement path for the portion of the protocol configuration hierarchy that configures the hello interval on an interface in an OSPF area.

The **protocols** statement is a top-level statement at the trunk of the configuration tree. The **ospf**, **area**, and **interface** statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree); and the **hello-interval** statement is a leaf on the tree which in this case contains a data value: the length of the hello interval, in seconds.

The CLI represents the statement path shown in [Figure 13](#) as **[edit protocols ospf area *area-number* interface *interface-name*]** and displays the configuration as follows:

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
      interface so-0/0/1 {
        hello-interval 5;
      }
    }
  }
}
```

The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed.

Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon.

The configuration hierarchy can also contain “oneliners” at the last level in the hierarchy. Oneliners remove one level of braces in the syntax and display the container statement, its identifiers, the child or leaf statement and its attributes all on one line. For example, in the following sample configuration hierarchy, the line **level 1 metric 10** is a oneliner because the **level** container statement with identifier **1**, its child statement **metric**, and its corresponding attribute **10** all appear on a single line in the hierarchy:

```
[edit protocols]
isis {
  interface ge-0/0/0.0 {
    level 1 metric 10;
  }
}
```

Likewise, in the following example, **dynamic-profile *dynamic-profile-name* aggregate-clients;** is a oneliner because the **dynamic-profile** statement, its identifier ***dynamic-profile-name***, and leaf statement **aggregate-clients** all appear on one line when you run the **show** command in the configuration mode:

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  dynamic-profile dynamic-profile-name aggregate-clients;
}
```

Related Documentation • [Entering and Exiting the Junos OS CLI Configuration Mode on page 462](#)

Entering and Exiting the Junos OS CLI Configuration Mode

You configure Junos OS by entering configuration mode and creating a hierarchy of configuration mode statements.

- To enter configuration mode, use the **configure** command.

When you enter configuration mode, the following configuration mode commands are available:

```
user@host>configure
entering configuration mode

[edit]
user@host#?
possible completions:
  <[Enter]>      Execute this command
  activate      Remove the inactive tag from a statement
  annotate      Annotate the statement with a comment
  commit        Commit current set of changes
  copy          Copy a statement
  deactivate    Add the inactive tag to a statement
  delete        Delete a data element
  edit          Edit a sub-element
  exit          Exit from this level
  help          Provide help information
  insert        Insert a new ordered data element
  load          Load configuration from ASCII file
  quit          Quit from this level
  rename        Rename a statement
  replace       Replace character string in configuration
  rollback      Roll back to previous committed configuration
  run           Run an operational-mode command
  save          Save configuration to ASCII file
  set           Set a parameter
  show          Show a parameter
  status        Show users currently editing configuration
  top           Exit to top level of configuration
  up            Exit one level of configuration
  wildcard      Wildcard operations
[edit]
user@host>
```

Users must have configure permission to view and use the **configure** command. When in configuration mode, a user can view and modify only those statements for which they have access privileges set. For more information, see the *Junos OS Administration Library for Routing Devices*.

- If you enter configuration mode and another user is also in configuration mode, a message shows the user's name and what part of the configuration the user is viewing or editing:

```
user@host> configure
Entering configuration mode
Users currently editing the configuration:
  root terminal d0 (pid 4137) on since 2008-04-09 23:03:07 PDT, idle 7w6d 08:22
```

```
[edit]
The configuration has been changed but not committed
```

```
[edit]
user@host#
```

Up to 32 users can be in configuration mode simultaneously, and they all can make changes to the configuration at the same time.

- To exit configuration mode, use the **exit configuration-mode** configuration mode command from any level, or use the **exit** command from the top level. For example:

```
[edit protocols ospf area 0.0.0.0 interface so-0/0/0]
user@host# exit configuration-mode
exiting configuration mode
user@host>

[edit]
user@host# exit
exiting configuration mode
user@host>
```

If you try to exit from configuration mode using the **exit** command and the configuration contains changes that have not been committed, you see a message and prompt:

```
[edit]
user@host# exit
The configuration has been changed but not committed
Exit with uncommitted changes? [yes,no] (yes) <Enter>
Exiting configuration mode
user@host>
```

- To exit with uncommitted changes without having to respond to a prompt, use the **exit configuration-mode** command. This command is useful when you are using scripts to perform remote configuration.

```
[edit]
user@host# exit configuration-mode
The configuration has been changed but not committed
Exiting configuration mode
user@host>
```

Related Documentation

- [Understanding Junos OS CLI Configuration Mode on page 456](#)

- [Modifying the Junos OS Configuration on page 468](#)
- [Commit Operation When Multiple Users Configure the Software on page 511](#)
- [Displaying the Current Junos OS Configuration on page 497](#)
- [Displaying set Commands from the Junos OS Configuration on page 501](#)
- [Issuing Relative Junos OS Configuration Mode Commands on page 475](#)
- [Using the configure exclusive Command on page 467](#)
- [Updating the configure private Configuration on page 496](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 431](#)

Notational Conventions Used in Junos OS Configuration Hierarchies

When you are working in Junos OS command-line interface (CLI) configuration mode, the banner on the line preceding the prompt indicates the current hierarchy level. In the following example, the level is **[edit protocols ospf]**:

```
[edit protocols ospf]  
user@host#
```

(The Junos OS documentation uses **user@host#** as the standard configuration mode prompt. In an actual CLI session, the prompt shows your user ID and the name of the Juniper Networks device you are working on.)

Use the **set ?** command to display the statements that you can include in the configuration at the current level. The **help apropos** command is also context-sensitive, displaying matching statements only at the current level and below.



NOTE: In this document, statements are listed alphabetically within each hierarchy and subhierarchy. If a subhierarchy is sufficiently long that it might be difficult to determine where it ends and its next peer statement begins, the subhierarchy appears at the end of its parent hierarchy instead of in alphabetical order. In this case, a placeholder appears in its actual alphabetical position.

For example, at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level, the family *family-name* subhierarchy has more than 20 child statements, including several subhierarchies with child statements of their own. The full family *family-name* hierarchy appears at the end of its parent hierarchy ([edit interfaces *interface-name* unit *logical-unit-number*]), and the following placeholder appears at its actual alphabetical position:

```
family family-name {
    ... the family subhierarchy appears after the main [edit interfaces interface-name
        unit logical-unit-number] hierarchy ...
}
```

Another exception to alphabetical order is that the **disable** statement always appears first in any hierarchy that includes it.

- Related Documentation**
- *Configuration Features in the Junos OS*
 - *Configuration Mode Commands in the Junos OS*

Forms of the configure Command

The Junos OS supports three forms of the **configure** command: **configure**, **configure private**, and **configure exclusive**. These forms control how users edit and commit configurations and can be useful when multiple users configure the software. See [Table 59](#).

Table 59: Forms of the configure Command

Command	Edit Access	Commit Access
configure	<ul style="list-style-type: none"> No one can lock the configuration. All users can make configuration changes. <p>When you enter configuration mode, the CLI displays the following information:</p> <ul style="list-style-type: none"> A list of other users editing the configuration. Hierarchy levels the users are viewing or editing. Whether the configuration has been changed, but not committed. When multiple users enter conflicting configurations, the most recent change to be entered takes precedence. 	<ul style="list-style-type: none"> No one can lock the configuration. All users can commit all changes to the configuration. If you and another user make changes and the other user commits changes, your changes are committed as well.
configure exclusive	<ul style="list-style-type: none"> One user locks the configuration and makes changes without interference from other users. Other users can enter and exit configuration mode, but they cannot commit the configuration. If you enter configuration mode while another user has locked the configuration (with the configure exclusive command), the CLI displays the user and the hierarchy level the user is viewing or editing. If you enter configuration mode while another user has locked the configuration, you can forcibly log out that user with the request system logout operational mode command. For details, see the CLI Explorer. 	
configure private	<ul style="list-style-type: none"> Multiple users can edit the configuration at the same time. Each user has a private candidate configuration to edit independently of other users. When multiple users enter conflicting configurations, the first commit operation takes precedence over subsequent commit operations. 	<ul style="list-style-type: none"> When you commit the configuration, the router verifies that the operational (running) configuration has not been modified by another user before accepting your private candidate configuration as the new operational configuration. If the configuration has been modified by another user, you can merge the modifications into your private candidate configuration and attempt to commit again.

Related Documentation

- [Committing a Junos OS Configuration on page 508](#)
- [Using the configure Command on page 468](#)
- [Displaying Users Currently Editing the Junos OS Configuration on page 504](#)
- [Using the configure exclusive Command on page 467](#)
- [Updating the configure private Configuration on page 496](#)
- [Displaying set Commands from the Junos OS Configuration on page 501](#)

Using the configure exclusive Command

If you enter configuration mode with the **configure exclusive** command, you lock the candidate *global* configuration (also known as the *shared configuration* or *shared configuration database*) for as long as you remain in configuration mode, allowing you to make changes without interference from other users. Other users can enter and exit configuration mode, but they cannot commit the configuration.

If another user has locked the configuration, and you need to forcibly log the person out, enter the operational mode command **request system logout pid *pid_number***.

If you enter configuration mode and another user is also in configuration mode and has locked the configuration, a message identifies the user and the portion of the configuration that the user is viewing or editing:

```
user@host> configure
Entering configuration mode
Users currently editing the configuration:
root terminal p3 (pid 1088) on since 2000-10-30 19:47:58 EDT, idle 00:00:44
exclusive [edit interfaces so-3/0/0 unit 0 family inet]
```

In configure exclusive mode, any uncommitted changes are discarded when you exit:

```
user@host> configure exclusive
warning: uncommitted changes will be discarded on exit
Entering configuration mode
[edit]
user@host# set system host-name cool
[edit]
user@host# quit
The configuration has been changed but not committed
warning: Auto rollback on exiting 'configure exclusive'
Discard uncommitted changes? [yes,no] (yes)
warning: discarding uncommitted changes
load complete
Exiting configuration mode
```

When you use the **yes** option to exit configure exclusive mode, Junos OS discards your uncommitted changes and rolls back your configuration. The **no** option allows you to continue editing or to commit your changes in configure exclusive mode.

When a user exits from configure exclusive mode while another user is in configure private mode, Junos OS will roll back any uncommitted changes.

- Related Documentation**
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
 - [Forms of the configure Command on page 465](#)

Using the configure Command

You can use the **configure** command to not only enter the CLI configuration mode but also to gather other information, such as other users currently in configuration mode.

Up to 32 users can be in configuration mode simultaneously, and they all can make changes to the configuration at the same time. When you commit changes to the configuration, you may be committing a combination of changes you and other users have made. For this reason, you will want to keep track on who if anyone is in configuration mode with you.

To see other users currently logged onto the same device in configuration mode:

- Use the **configure** command to enter the CLI configuration mode.

If there are other users, the message displayed indicates who the users are and what portion of the configuration the each person is viewing or editing.

```
user@host> configure
Entering configuration mode
Current configuration users:
root terminal p3 (pid 1088) on since 1999-05-13 01:03:27 EDT
[edit interfaces so-3/0/0 unit 0 family inet]
The configuration has been changed but not committed
[edit]
user@host#
```

Notice also that If, when you enter configuration mode, the configuration contains changes that have not been committed, another message is displayed:

```
user@host> configure
Entering configuration mode
The configuration has been changed but not committed
[edit]
user@host#
```

This tells you that another user has already made changes to the configuration.

- Related Documentation**
- [Forms of the configure Command on page 465](#)

Modifying the Junos OS Configuration

To configure a device running Junos OS or to modify an existing Junos OS configuration, you add statements to the configuration. For each statement hierarchy, you create the hierarchy starting with a statement at the top level and continuing with statements that move progressively lower in the hierarchy.

To modify the hierarchy, you use two configuration mode commands:

- **edit**—Moves to a particular hierarchy level. If that hierarchy level does not exist, the **edit** command creates it. The **edit** command has the following syntax:

```
edit <statement-path>
```

- **set**—Creates a configuration statement and sets identifier values. After you issue a **set** command, you remain at the same level in the hierarchy. The **set** command has the following syntax:

```
set <statement-path> statement <identifier>
```

statement-path is the hierarchy to the configuration statement and the statement itself. If you have already moved to the statement's hierarchy level, you can omit the statement path. **statement** is the configuration statement itself. **identifier** is a string that identifies an instance of a statement.

You cannot use the **edit** command to change the value of identifiers. You must use the **set** command.

Related Documentation

- [Displaying the Current Junos OS Configuration on page 497](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Using the configure exclusive Command on page 467](#)
- [Updating the configure private Configuration on page 496](#)
- [Issuing Relative Junos OS Configuration Mode Commands on page 475](#)

Adding Junos OS Configuration Statements and Identifiers

All properties of a device running Junos OS are configured by including *statements* in the configuration. A statement consists of a keyword, which is fixed text, and, optionally, an *identifier*. An identifier is an identifying name which you define, such as the name of an interface or a username, and which allows you and the CLI to discriminate among a collection of statements.

For example, the following list shows the statements available at the top level of configuration mode:

```
user@host# set?
Possible completions:
> accounting-options  Accounting data configuration
+ apply-groups        Groups from which to inherit configuration data
> chassis             Chassis configuration
> class-of-service    Class-of-service configuration
> firewall            Define a firewall configuration
> forwarding-options  Configure options to control packet sampling
> groups              Configuration groups
> interfaces          Interface configuration
> policy-options      Routing policy option configuration
> protocols           Routing protocol configuration
> routing-instances   Routing instance configuration
> routing-options     Protocol-independent routing option configuration
> snmp               Simple Network Management Protocol
> system              System parameters
```

An angle bracket (>) before the statement name indicates that it is a container statement and that you can define other statements at levels below it. If there is no angle bracket (>) before the statement name, the statement is a leaf statement; you cannot define other statements at hierarchy levels below it.

A plus sign (+) before the statement name indicates that it can contain a set of values. To specify a set, include the values in brackets. For example:

```
[edit]
user@host# set policy-options community my-as1-transit members [65535:10 65535:11]
```

In some statements, you can include an identifier. For some identifiers, such as interface names, you must specify the identifier in a precise format. For example, the interface name so-0/0/0 refers to a SONET/SDH interface that is on the Flexible PIC Concentrator (FPC) in slot 0, in the first PIC location, and in the first port on the Physical Interface Card (PIC). For other identifiers, such as interface descriptive text and policy and firewall term names, you can specify any name, including special characters, spaces, and tabs.

You must enclose in quotation marks (double quotes) identifiers and any strings that include a space or tab character or any of the following characters:

() [] { } ! @ # \$ % ^ & | ' = ?

If you do not type an option for a statement that requires one, a message indicates the type of information required. In this example, you need to type an area number to complete the command:

```
[edit]
user@host# set protocols ospf area<Enter>
^
syntax error, expecting <identifier>
```

Related Documentation

- [Modifying the Junos OS Configuration on page 468](#)
- [Deleting a Statement from a Junos OS Configuration on page 470](#)
- [Copying a Junos OS Statement in the Configuration on page 473](#)
- [Renaming an Identifier in a Junos OS Configuration on page 476](#)
- [Using the configure exclusive Command on page 467](#)
- [Additional Details About Specifying Junos OS Statements and Identifiers on page 541](#)
- [Displaying the Current Junos OS Configuration on page 497](#)

Deleting a Statement from a Junos OS Configuration

To delete a statement or identifier from a Junos OS configuration, use the **delete** configuration mode command. Deleting a statement or an identifier effectively "unconfigures" the functionality associated with that statement or identifier, returning that functionality to its default condition.

```
user@host# delete <statement-path> <identifier>
```

When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration.

For statements that can have more than one identifier, when you delete one identifier, only that identifier is deleted. The other identifiers in the statement remain.

To delete the entire hierarchy starting at the current hierarchy level, do not specify a statement or an identifier in the **delete** command. When you omit the statement or identifier, you are prompted to confirm the deletion:

```
[edit]
user@host# delete
Delete everything under this level? [yes, no] (no)
Possible completions:
no    Don't delete everything under this level
yes   Delete everything under this level
Delete everything under this level? [yes, no] (no)
```



NOTE: You cannot delete multiple statements or identifiers within a hierarchy using a single delete command. You must delete each statement or identifier individually using multiple delete commands. For example, consider the following configuration at the [edit system] hierarchy level:

```
system {
  host-name host-211;
  domain-name domain-122;
  backup-router 192.168.71.254;
  arp;
  authentication-order [ radius password tacplus ];
}
```

To delete the domain-name, host-name, and backup-router from the configuration, you cannot issue a single delete command:

```
user@host> delete system hostname host-211 domain-name domain-122 backup-router
192.168.71.254
```

You can only delete each statement individually:

```
user@host delete system host-name host-211
user@host delete system domain-name domain-122
user@host delete system backup-router 192.168.71.254
```

Related Documentation

- [Example: Deleting a Statement from the Junos OS Configuration on page 471](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Copying a Junos OS Statement in the Configuration on page 473](#)

Example: Deleting a Statement from the Junos OS Configuration

The following example shows how to delete the **ospf** statement, effectively unconfiguring OSPF on the router:

```
[edit]
```

```

user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
        hello-interval 5;
      }
    }
  }
}
[edit]
user@host# delete protocols ospf
[edit]
user@host# show
[edit]
user@host#

```

Delete all statements from the current level down:

```

[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# set interface so-0/0/0 hello-interval 5
[edit protocols ospf area 0.0.0.0]
user@host# delete
Delete everything under this level? [yes, no] (no) yes
[edit protocols ospf area 0.0.0.0]
user@host# show
[edit]
user@host#

```

Unconfigure a particular property:

```

[edit]
user@host# set interfaces so-3/0/0 speed 100mb
[edit]
user@host# show
interfaces {
  so-3/0/0 {
    speed 100mb;
  }
}
[edit]
user@host# delete interfaces so-3/0/0 speed
[edit]
user@host# show
interfaces {
  so-3/0/0;
}

```

- [Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608](#)
- [Deleting a Statement from a Junos OS Configuration on page 470](#)

Copying a Junos OS Statement in the Configuration

When you have many similar statements in a Junos configuration, you can add one statement and then make copies of that statement. Copying a statement duplicates that statement and the entire hierarchy of statements configured under that statement. Copying statements is useful when you are configuring many physical or logical interfaces of the same type.

To make a copy of an existing statement in the configuration, use the configuration mode **copy** command:

```
user@host# copy existing-statement to new-statement
```

Immediately after you have copied a portion of the configuration, the configuration might not be valid. You must check the validity of the new configuration, and if necessary, modify either the copied portion or the original portion for the configuration to be valid.

Related Documentation

- [Example: Copying a Statement in the Junos Configuration on page 473](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Examples: Re-Using Configuration on page 476](#)

Example: Copying a Statement in the Junos Configuration

This example shows how you can create one virtual connection (VC) on an interface by copying an existing VC.

- [Requirements on page 473](#)
- [Overview on page 474](#)
- [Configuration on page 474](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Before you begin this example, configure the following initial configuration.

```
[edit interfaces]
user@host# show
at-1/0/0 {
  description "PAIX to MAE West"
  encapsulation atm-pvc;
  unit 61 {
    point-to-point;
    vci 0.61;
    family inet {
      address 10.0.1.1/24;
    }
  }
}
```

To quickly configure the *initial configuration* for this example, copy the following commands, paste it into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste this command into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces at-1/0/0 description "PAIX to MAE West"
set interfaces at-1/0/0 encapsulation atm-pvc
set interfaces at-1/0/0 unit 61 point-to-point
set interfaces at-1/0/0 unit 61 vci 0.61
set interfaces at-1/0/0 unit 61 family inet address 10.0.1.1/24
```

Overview

Copying statements is useful when you are configuring many physical or logical interfaces of the same type. You can add one statement and then make copies of that statement. Copying a statement duplicates that statement and the entire hierarchy of statements configured under that statement. In the case of this example, we are adding a virtual connection that is very similar to a virtual connection already configured.

Configuration

CLI Quick Configuration

Start at the **[edit interfaces at-1/0/0]** hierarchy level.

```
copy unit 61 to unit 62
set unit 62 vci 0.62
edit unit 62
replace pattern 10.0.1.1 with 10.0.2.1
```

Configuring by Copying

Step-by-Step Procedure

To configure by copying a configuration:

1. Go to the **[edit interfaces at-1/0/0]** hierarchy level and copy unit 61.

```
[edit interfaces at-1/0/0]
user@host# copy unit 61 to unit 62
```

2. Take a look at the new configuration and see what you need to change to make the configuration valid..

```
user@host# show interfaces at-1/0/0
description "PAIX to MAE West"
encapsulation atm-pvc;
unit 61 {
  point-to-point;
  vci 0.61;
  family inet {
    address 10.0.1.1/24;
  }
}
unit 62 {
  point-to-point;
  vci 0.61;
  family inet {
    address 10.0.1.1/24;
  }
}
```

```
}
```

3. Change the configuration to make it valid.

In this example you want to reconfigure the virtual circuit identifier (VCI) and virtual path identifier (VPI).

```
[edit interfaces at-1/0/0]
user@host# set unit 62 vci 0.62
```

You also want to replace the IP address of the new interface with its own IP address.

```
[edit interfaces at-1/0/0]
user@host# edit unit 62
user@host# replace pattern 10.0.1.1 with 10.0.2.1
```

Results

```
[edit]
show interfaces
at-1/0/0 {
  description "PAIX to MAE West"
  encapsulation atm-pvc;
  unit 61 {
    point-to-point;
    vci 0.61;
    family inet {
      address 10.0.1.1/24;
    }
  }
  unit 62 {
    point-to-point;
    vci 0.62;
    family inet {
      address 10.0.2.1/24;
    }
  }
}
```

Related Documentation • [Copying a Junos OS Statement in the Configuration on page 473](#)

Issuing Relative Junos OS Configuration Mode Commands

The **top** or **up** command followed by another configuration command, including **edit**, **insert**, **delete**, **deactivate**, **annotate**, or **show** enables you to quickly move to the top of the hierarchy or to a level above the area you are configuring.

To issue configuration mode commands from the top of the hierarchy, use the **top** command; then specify a configuration command. For example:

```
[edit interfaces fxp0 unit 0 family inet]
user@host# top edit system login
[edit system login]
user@host#
```

To issue configuration mode commands from a location higher up in the hierarchy, use the **up** configuration mode command; specify the number of levels you want to move up the hierarchy and then specify a configuration command. For example:

```
[edit protocols bgp]
user@host# up 2 activate system
```

**Related
Documentation**

- [Displaying the Current Junos OS Configuration on page 497](#)

Renaming an Identifier in a Junos OS Configuration

When modifying a Junos configuration, you can rename an identifier that is already in the configuration. You can do this either by deleting the identifier (using the **delete** command) and then adding the renamed identifier (using the **set** and **edit** commands), or you can rename the identifier using the **rename** configuration mode command:

```
user@host# rename <statement-path> identifier1 to identifier2
```

**Related
Documentation**

- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Examples: Re-Using Configuration on page 476](#)
- [Inserting a New Identifier in a Junos OS Configuration on page 481](#)

Examples: Re-Using Configuration

If you need to make changes to the configuration of a device, you can always remove the original configuration settings using the **delete** command and add your new configuration settings using the **set** command. There are, however, other ways of modifying a configuration that are more efficient and easier to use.

This example shows how to use the following configuration mode commands to update an existing configuration:

- **rename**—Rename an existing configuration setting, such as an interface name. This can be useful when you are adding new interfaces to a device.
 - **copy**—Copy a configuration setting and the entire hierarchy of statements configured under that setting. Copying configuration statements is useful when you are configuring many physical or logical interfaces of the same type.
 - **replace**—Make global changes to text patterns in the configuration. For example, if you consistently misspell a word common to the description statement for all of the interfaces on your device, you can fix this mistake with a single command.
- [Requirements on page 477](#)
 - [Overview on page 477](#)
 - [Configuration on page 477](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

In the course of the first example in this topic, you will make the following configuration changes:

- Create a new interface with a description that contains a typing error.
- Copy the configuration from the interface that you created to create a new interface.
- Rename one of the interfaces that you created.
- Fix the typing error in the description for the interfaces that you created.

In the second, shorter example, you will experiment with some of the same commands under slightly different circumstances.

Configuration

CLI Quick Configuration

This example does not use commands that are suitable for this section.

Using the Copy, Rename, and Replace Commands to Modify a Loopback Interface Configuration

Step-by-Step Procedure



CAUTION: If your configuration uses any of the loopback interface unit numbers used in this example, you must substitute different loopback interface unit numbers that you are not using in your device's configuration in the following steps to avoid adversely impacting the operational status of your device.

To create and modify a configuration of a loopback interface using the **copy**, **rename**, and **replace** commands:

1. Create a new loopback interface unit number and include a description.
The mistakes in the spelling of *loopback* in the description are intentional.
[edit]
user@host# **set interfaces lo0 unit 100 description "this is a lopbck interface"**
2. Display the configuration for the loopback interface you have just added.
[edit]
user@host# **show interfaces lo0 unit 100 description "this is a lopbck interface";**
3. Duplicate the loopback interface you have just created, warts and all, from unit 100 to unit 101.

```
[edit]
user@host# copy interfaces lo0 unit 100 to unit 101
```

4. Display the configurations for loopback interfaces lo0 unit 100 and lo0 unit 101.

```
[edit]
user@host# show interfaces lo0 unit 100
description "this is a lopbck interface";
[edit]
user@host# show interfaces lo0 unit 101
description "this is a lopbck interface";
```

The **copy** command duplicates an interface including any child statements such as **description**.

5. Rename the loopback interface lo0 unit 100 to loopback interface lo0 unit 102.

```
[edit]
user@host# rename interfaces lo0 unit 100 to unit 102
```

6. Display the configuration for loopback interface lo0 unit 100.

```
[edit]
user@host# show interfaces lo0 unit 100
[edit]
user@host#
```

You should not see any results from this command. The loopback interface lo0 unit 100 is now gone. The **rename** command replaces the configuration statement indicated with the new configuration.

7. Fix the misspelling of the word *loopback* in the descriptions for loopback interfaces lo0 unit 101 and lo0 unit 102.

```
[edit]
user@host# replace pattern lopbck with loopback
```

8. Display the configuration for loopback interfaces lo0 unit 101 and lo0 102 to verify that the word *loopback* is spelled correctly now.

```
[edit]
user@host# show interfaces lo0 unit 101
description "this is a loopback interface";
[edit]
user@host# show interfaces lo0 unit 102
description "this is a loopback interface";
```

The **replace** command replaces all instances of the pattern specified in the command, unless limited in some way. The next example in this topic shows one way to limit the effect of the **replace** command.

9. From configuration mode, use the **rollback** command to put the device's configuration back to the state it was in before you executed the previous steps.

```
[edit]
user@host# rollback
```

Results From configuration mode, use the **show interfaces lo0 unit 101** and **show interfaces lo0 unit 102** commands to ensure that the device's configuration is back to the state it was in before you executed the steps in this example.

```
[edit]
user@host: show interfaces lo0 unit 101
[edit]
user@host#
```

You should not see any results from this command.

```
[edit]
user@host# show interfaces lo0 unit 102
[edit]
user@host#
```

You should not see any results from this command.

Compare the Copy Command at the Top-Level Configuration Hierarchy Level

Step-by-Step Procedure The previous example shows the **copy**, **rename**, and **replace** commands at the **[edit interfaces interface-name unit logical-interface-number]** hierarchy level. This example shows how some of these commands work at the top level of the CLI configuration mode hierarchy.

The following example requires you to navigate to various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

1. Create an Ethernet interface.

```
[edit]
user@host# set interfaces et-2/0/0 unit 0 family inet address 192.0.2.2
```

2. Copy the interface you just created to another interface.

```
[edit]
user@host# copy interfaces et-2/0/0 to et-2/1/0
```

Compare this **copy** command to the one in Step 3 in the first example, where the **copy** command takes the keyword **unit** before the value to be copied. Notice that the keyword **interfaces** is not repeated after the preposition **to** and before the value to be copied. This happens in some top-level statements with the **copy** command.



TIP: Similarly, in the **rename** command, you do not repeat the keyword part of the statement before the new identifier in some top-level statements.

3. Show your configuration so far.

```
[edit]
user@host# show interfaces
et-2/0/0 {
  unit 0 {
```

```
        family inet {
            address 192.0.2.2/32;
        }
    }
}
et-2/1/0 {
    unit 0 {
        family inet {
            address 192.0.2.2/32;
        }
    }
}
```

4. Replace the address for et-2/1/0 with another IP address.

```
[edit interfaces et-2/1/0 unit 0 family inet]
user@host# replace pattern 192.0.2.2 with 192.0.2.40
```

Notice that if you want to change only a specific occurrence of a pattern instead of all of them (as you did in Step 7 in the first example), you need to drill down to that specific hierarchy level before using the **replace** command.

5. Show your interfaces again.

```
[edit]
user@host# show interfaces
et-2/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.2/32;
        }
    }
}
et-2/1/0 {
    unit 0 {
        family inet {
            address 192.0.2.40/32;
        }
    }
}
```

6. From configuration mode, use the **rollback** command to put the device's configuration back to the state it was in before you executed the previous steps.

```
[edit]
user@host# rollback
```

Results From configuration mode, use the **show interfaces et-2/0/0** and **show interfaces et-2/1/0** commands to ensure that the device's configuration is back to the state it was in before you executed the steps in this example.

```
[edit]
user@host# show interfaces et-2/0/0
[edit]
user@host#
```

You should not see any results from this command.


```
[edit]
user@R1# show interfaces et-2/1/0
[edit]
user@host#
```

You should not see any results from this command.

Related Documentation

- [rename on page 683](#)
- [replace on page 684](#)
- [Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference on page 604](#)
- [Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608](#)
- [Copying a Junos OS Statement in the Configuration on page 473](#)
- [Example: Copying a Statement in the Junos Configuration on page 473](#)

Inserting a New Identifier in a Junos OS Configuration

When configuring a device running Junos OS, you can enter most statements and identifiers in any order. Regardless of the order in which you enter the configuration statements, the CLI always displays the configuration in a strict order. However, there are a few cases where the ordering of the statements matters because the configuration statements create a sequence that is analyzed in order.

For example, in a routing policy or firewall filter, you define terms that are analyzed sequentially. Also, when you create a named path in dynamic MPLS, you define an ordered list of the transit routers in the path, starting with the first transit router and ending with the last one.

To modify a portion of the configuration in which the statement order matters, use the **insert** configuration mode command:

```
user@host# insert <statement-path> identifier1 (before | after) identifier2
```

If you do not use the **insert** command, but instead simply configure the identifier, it is placed at the end of the list of similar identifiers.

Related Documentation

- [Renaming an Identifier in a Junos OS Configuration on page 476](#)
- [Examples: Re-Using Configuration on page 476](#)
- [Example: Inserting a New Identifier in a Junos Configuration on page 481](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489](#)

Example: Inserting a New Identifier in a Junos Configuration

This example shows the use of the **insert** command.

Whereas a term added using the **set** command is placed at the end of the existing list of terms, you use the **insert** command to add a term in the order you specify. Specifying the order of statement is important in the cases in which the order of the statements matters because the configuration statements create a sequence that is analyzed in order.

Also notice, as shown in this example, that you must create the term before you can place it using the **insert** command.

- [Requirements on page 482](#)
- [Overview on page 483](#)
- [Configuration on page 483](#)

Requirements

Before you can insert a term, you must configure an initial policy. To quickly configure the initial policy for this example, copy the following commands, paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit policy-options]** hierarchy level, and then enter **commit** from configuration mode.

```
set policy-statement statics term term1 from route-filter 192.168.0.0/16 orlonger
set policy-statement statics term term1 from route-filter 224.0.0.0/3 orlonger
set policy-statement statics term term1 then reject
set policy-statement statics term term2 from protocol direct
set policy-statement statics term term2 then reject
set policy-statement statics term term3 from protocol static
set policy-statement statics term term3 then reject
set policy-statement statics term term4 then accept
```

Now check that you have the hierarchy correctly configured.

```
[edit policy-options]
user@host# show
policy-statement statics {
  term term1 {
    from {
      route-filter 192.168.0.0/16 orlonger;
      route-filter 224.0.0.0/3 orlonger;
    }
    then reject;
  }
  term term2 {
    from protocol direct;
    then reject;
  }
  term term3 {
    from protocol static;
    then reject;
  }
  term term4 {
    then accept;
  }
}
```

Overview

When configuring a device running Junos OS, you can enter most statements and identifiers in any order. However, there are a few cases, such as in routing policies or firewall filters, in which the order of the statements matters because the configuration statements create a sequence that is analyzed in order.

To modify a portion of the configuration in which the statement order matters, you must use the **insert** configuration mode command. If you use the **set** command instead, the added statement or identifier will be in the wrong place sequentially. The only other way to get the terms of the command in the correct order is to dismantle the configuration and start over.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit policy-options] hierarchy level, and then enter commit from configuration mode.

```
[edit]
user@host# rename policy-options policy-statement statics term term4 to term term6
[edit]
user@host# set policy-options policy-statement statics term term4 from protocol local
[edit]
user@host# set policy-options policy-statement statics term term4 then reject
[edit]
user@host# set policy-options policy-statement statics term term5 from protocol
aggregate
[edit]
user@host# set policy-options policy-statement statics term term5 then reject
[edit]
user@host# insert policy-options policy-statement statics term term4 after term term3
[edit]
user@host# insert policy-options policy-statement statics term term5 after term term4
```

Configuring to Insert Terms

Step-by-Step Procedure

1. Determine in what order the terms in your configuration need to go—the original terms and the new terms you plan to add.

In the original configuration, the policy is named **statics** and there are four terms. Each of the first three terms matches on a different match criteria and the resulting matches are rejected. The last term accepts all the rest of the traffic.

In this example, you need to add two terms that weed out additional types of traffic. Both of these terms need to go before the last term in the original configuration.

2. Rename original term4 to term6.

```
[edit]
user@host# rename policy-options policy-statement statics term term4 to term
term6
```

This step preserves the original last term, now renamed term6, as the last term.

3. Create a new term4.

```
[edit]
user@host# set policy-options policy-statement statics term term4 from protocol
local
user@host# set policy-options policy-statement statics term term4 then reject
```

A new term is added that matches traffic from local system addresses and rejects it.

4. Create new term5.

```
[edit]
user@host# set policy-options policy-statement statics term term5 from protocol
aggregate
user@host# set policy-options policy-statement statics term term5 then reject
```

A new term is added that matches traffic from aggregate routes and rejects it.

5. Insert term4 after term3.

```
[edit]
user@host# insert policy-options policy-statement statics term term4 after term
term3
```

6. Insert term5 after term4.

```
[edit]
user@host# insert policy-options policy-statement statics term term5 after term
term4
```

Results

```
[edit]
user@host# show policy-options policy-statement statics
term term1 {
  from {
    route-filter 192.168.0.0/16 orlonger;
    route-filter 224.0.0.0/3 orlonger;
  }
  then reject;
}
term term2 {
  from protocol direct;
  then reject;
}
term term3 {
  from protocol static;
  then accept;
}
term term4 {
  from protocol local;
  then reject;
}
term term5 {
  from protocol aggregate;
  then reject;
}
```

```
term term6 {
  then accept;
}
```

Related Documentation

- [Inserting a New Identifier in a Junos OS Configuration on page 481](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)

Example: Using the Wildcard Command with the Range Option

- [Requirements on page 485](#)
- [Overview on page 485](#)
- [Configuration on page 486](#)
- [Verification on page 488](#)

Requirements

This example uses the following hardware and software components:

- M Series, MX Series, T Series or EX Series device
- Junos OS Release 12.1 or later running on the device

Overview

The **range** option with the **wildcard** command enables you to specify ranges in **activate**, **deactivate**, **delete**, **protect**, **set**, **show**, and **unprotect** commands. You can use ranges to specify a range of interfaces, logical units, VLANs, and other numbered elements. The **wildcard range** option expands the command you entered into multiple commands, each of which corresponds to one item in the range.

The **wildcard range** option enables you to configure multiple configuration statements using a single **set** command, instead of configuring each of them individually. For example, to configure 24 Gigabit Ethernet interfaces with different port numbers, you can use a single **wildcard range set** command instead of 24 individual **set interfaces** commands.

Similarly, to deactivate a group of 30 logical interfaces, you can use the **wildcard range deactivate** command instead of deactivating each logical interface individually.

You can use **wildcard range** with the **active**, **deactivate**, **delete**, **protect**, **set**, **show**, and **unprotect** configuration commands:

```
user@host# wildcard range ?
```

Possible completions:

activate	Remove the inactive tag from a statement
deactivate	Add the inactive tag to a statement
delete	Delete a data element
protect	Protect the statement
set	Set a parameter
show	Show a parameter
unprotect	Unprotect the statement

You can also specify all configuration hierarchy levels and their child configuration statements in the CLI by using **wildcard range** with the **set** option:

Possible completions:

```
> > access           Network access configuration
> > access-profile    Access profile for this instance
> > accounting-options Accounting data configuration
> > applications      Define applications by protocol characteristics
...
```

Configuration

The following examples show how to configure multiple configuration statements in a single step by using the **range** option with the **wildcard** configuration command:

- [Using the Range Option for Configuring a Series of Named Identifiers for a Configuration Statement on page 486](#)
- [Specifying Multiple Ranges in the Syntax on page 486](#)
- [Specifying a Range and Unique Numbers In the Syntax on page 487](#)
- [Excluding Some Values from a Range on page 487](#)
- [Specifying a Range with a Step Number on page 488](#)

Using the Range Option for Configuring a Series of Named Identifiers for a Configuration Statement

Step-by-Step Procedure

You can configure a series of identifiers for a configuration statement, by specifying a numerical range of values for the identifiers.

- To configure a series of the same type of interface with different port numbers (0 through 23), specify the range for the port numbers by using the following format:

```
[edit]
user@host# wildcard range set interfaces ge-0/0/[0-23] unit 0 family vpls
```

Results Expands to 24 different **set** commands to configure interfaces with port numbers ranging from 0 through 23:

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family vpls
user@host# set interfaces ge-0/0/1 unit 0 family vpls
user@host# set interfaces ge-0/0/2 unit 0 family vpls
...
user@host# set interfaces ge-0/0/23 unit 0 family vpls
```

Specifying Multiple Ranges in the Syntax

Step-by-Step Procedure

You can have multiple ranges specified in a **wildcard range** command. Each range must be separated by a comma. You can also have overlapping ranges.

- To specify more than one range in the syntax, include the minimum and maximum values for each range, separated by a comma.

```
[edit]
```

```
user@host# wildcard range protect event-options policy p[1-3,5-7,6-9]
```

Results Expands to the following **set** commands:

```
[edit]
user@host# set protect event-options policy p1
user@host# set protect event-options policy p2
user@host# set protect event-options policy p3
user@host# set protect event-options policy p5
user@host# set protect event-options policy p6
user@host# set protect event-options policy p7
user@host# set protect event-options policy p8
user@host# set protect event-options policy p9
```

Specifying a Range and Unique Numbers In the Syntax

Step-by-Step Procedure You can also specify a combination of a range and unique numbers in the syntax of the **wildcard range** command.

- To specify a range and unique numbers, separate them with a comma.

```
[edit]
user@host# wildcard range protect event-options policy p[1-3,5,7,10]
```

Results Expands to the following **set** commands:

```
[edit]
user@host# set protect event-options policy p1
user@host# set protect event-options policy p2
user@host# set protect event-options policy p3
user@host# set protect event-options policy p5
user@host# set protect event-options policy p7
user@host# set protect event-options policy p10
```

Excluding Some Values from a Range

Step-by-Step Procedure You can exclude certain values from a range by marking the numbers or the range of numbers to be excluded by using an exclamation mark.

- To exclude certain values from a range, include the portion to be excluded with **!** in the syntax.

```
[edit]
user@host# wildcard range protect event-options policy p[1-5,!3-4]
```

Results Expands to the following **set** commands:

```
[edit]
user@host# set protect event-options policy p1
user@host# set protect event-options policy p2
user@host# set protect event-options policy p5
```

Specifying a Range with a Step Number

- Step-by-Step Procedure** You can provide a step number for a range to have a constant interval in the range.
- To provide a step, include the step value in the syntax preceded by a forward slash (/).
- ```
[edit]
user@host# wildcard range protect event-options policy p[1-10/2]
```

**Results** Expands to the following **set** commands:

```
[edit]
user@host# set protect event-options policy p1
user@host# set protect event-options policy p3
user@host# set protect event-options policy p5
user@host# set protect event-options policy p7
user@host# set protect event-options policy p9
```

### Verification

Confirm that the configuration is working properly.

- [Checking the Configuration on page 488](#)

### Checking the Configuration

---

**Purpose** Check the configuration created using the **wildcard range** option. The following sample shows output for the configuration described in “[Using the Range Option for Configuring a Series of Named Identifiers for a Configuration Statement](#)” on page 486.



**Action** user@host> show configuration interfaces

```

ge-0/0/0 {
 unit 0 {
 family vpls;
 }
}
ge-0/0/1 {
 unit 0 {
 family vpls;
 }
}
ge-0/0/2 {
 unit 0 {
 family vpls;
 }
}
ge-0/0/3 {
 unit 0 {
 family vpls;
 }
}
...
ge-0/0/23 {
 unit 0 {
 family vpls;
 }
}

```

**Meaning** The output indicates that 24 Gigabit Ethernet interfaces ranging from **ge-0/0/0** through **ge-0/0/23** are created.

**Related Documentation** • [Using Wildcard Characters in Interface Names on page 601](#)

## Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration

In a Junos configuration, you can deactivate statements and identifiers so that they do not take effect when you issue the **commit** command. Any deactivated statements and identifiers are marked with the **inactive** tag. They remain in the configuration, but are not activated when you issue a **commit** command.

To deactivate a statement or identifier, use the **deactivate** configuration mode command:

```
user@host# deactivate(statement | identifier)
```

To reactivate a statement or identifier, use the **activate** configuration mode command:

```
user@host# activate (statement | identifier)
```

In both commands, the **statement** and **identifier** you specify must be at the current hierarchy level. When you deactivate a statement, that specific statement is completely ignored and is not applied at all when you issue a **commit** command.

To disable a statement, use the **disable** configuration mode command:

In some portions of the configuration hierarchy, you can include a **disable** statement to disable functionality. One example is disabling an interface by including the **disable** statement at the **[edit interface *interface-name*]** hierarchy level. When you disable a functionality, it is activated when you issue a **commit** command but is treated as though it is down or administratively disabled.

**Related  
Documentation**

- [Example: Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 490](#)
- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)

---

## Example: Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration

---

This example shows a common use case in which the **deactivate** and **activate** configuration mode commands are used. It involves dual Routing Engines, master and backup, that have graceful Routing Engine switchover (GRES) configured. The software on both Routing Engines needs to be upgraded. This can easily be accomplished by deactivating GRES, updating the Routing Engines, and then reactivating GRES.



**NOTE:** You can also perform a similar upgrade using the same setup except that nonstop active routing (NSR) is configured instead of GRES. You would need to deactivate NSR and then upgrade the Routing Engines before reactivating NSR.

- 
- [Requirements on page 490](#)
  - [Overview on page 490](#)
  - [Configuration on page 491](#)

### Requirements

This example requires the use of a router with dual Routing Engines that can be upgraded.

Before you begin this example, make sure that you have GRES configured.

### Overview

In this example, there are two Routing Engines. GRES is configured, and the Routing Engines need to be upgraded. To accomplish the upgrading, you need to deactivate the GRES feature, upgrade each of the Routing Engines, and then activate GRES again.

## Configuration

### Configuring the Deactivation and Reactivation of GRES

#### Step-by-Step Procedure

To deactivate and reactivate GRES for Routing Engine upgrade:

1. Show that GRES is enabled for the router.

```
[edit]
user@host# show chassis
redundancy {
 graceful-switchover;
}
fpc 2 {
 pic 0 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}
```

2. Deactivate GRES.

```
[edit]
user@host# deactivate chassis redundancy graceful-switchover
user@host# commit
```

3. Show that GRES is deactivated.

```
[edit]
user@host# show chassis
redundancy {
 inactive: graceful-switchover;
}
fpc 2 {
 pic 0 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}
```

4. Upgrade the Routing Engines one by one.

For instructions on upgrading Junos OS on dual Routing Engines, see tasks 2 and 3 in [“Installing the Software Package on a Router with Redundant Routing Engines” on page 58](#).

5. Reactivate GRES.

```
[edit]
user@host# activate chassis redundancy graceful-switchover
user@host# commit
```

**Results** Verify that GRES feature is activated again.

```
[edit]
user@host# show chassis
```

```
redundancy {
 graceful-switchover;
}
fpc 2 {
 pic 0 {
 tunnel-services {
 bandwidth 1g;
 }
 }
}
```

**Related Documentation**

- [Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489](#)

---

## Adding Comments in a Junos OS Configuration

You can include comments in a Junos configuration to describe any statement in the configuration. You can add comments interactively in the CLI and by editing the ASCII configuration file.

When configuring interfaces, you can add comments about the interface by including the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level. Any comments you include appear in the output of the **show interfaces** commands. For more information about the **description** statement, see the *Junos OS Network Interfaces Library for Routing Devices*.

- [Adding Comments in the CLI on page 492](#)
- [Adding Comments in a File on page 493](#)

### Adding Comments in the CLI

When you add comments in configuration mode, they are associated with a statement at the current level. Each statement can have one single-line comment associated with it. Before you can associate a comment with a statement, the statement must exist. The comment is placed on the line preceding the statement.

To add comments to a configuration, use the **annotate** configuration mode command:

```
user@host# annotate statement "comment-string"
```

***statement*** is the configuration statement to which you are attaching the comment; it must be at the current hierarchy level. If a comment for the specified ***statement*** already exists, it is deleted and replaced with the new comment.

***comment-string*** is the text of the comment. The comment text can be any length, and you must type it on a single line. If the comment contains spaces, you must enclose it in quotation marks. In the comment string, you can include the comment delimiters ***/\* \*/*** or ***#***. If you do not specify any, the comment string is enclosed with the ***/\* \*/*** comment delimiters.

To delete an existing comment, specify an empty comment string:

```
user@host# annotate statement ""
```

If you add comments with the **annotate** command, you can view the comments within the configuration by entering the **show** configuration mode command or the **show configuration** operational mode command.



**NOTE:** The Junos OS supports annotation up to the last level in the configuration hierarchy, including oneliners. However, annotation of parts (the child statements or identifiers within the oneliner) of the oneliner is not supported. For example, in the following sample configuration hierarchy, annotation is supported up to the level 1 parent hierarchy, but not supported for the metric child statement:

```
[edit protocols]
 isis {
 interface ge-0/0/0.0 {
 level 1 metric 10;
 }
 }
}
```

## Adding Comments in a File

When you edit the ASCII configuration file and add comments, they can be one or more lines and must precede the statement they are associated with. If you place the comments in other places in the file, such as on the same line following a statement or on a separate line following a statement, they are removed when you use the **load** command to open the configuration into the CLI.

The following excerpt from a configuration example illustrates how to place and how not to place comments in a configuration file:

```
/* This comment goes with routing-options */
routing-options {
 /* This comment goes with routing-options traceoptions */
 traceoptions {
 /* This comment goes with routing-options traceoptions tracefile */
 tracefile rpd size 1m files 10;
 /* This comment goes with routing-options traceoptions traceflag task */
 traceflag task;
 /* This comment goes with routing-options traceoptions traceflag general */
 traceflag general;
 }
 autonomous-system 10458; /* This comment is dropped */
}
routing-options {
 rib-groups {
 ifrg {
 import-rib [inet.0 inet.2];
 /* A comment here is dropped */
 }
 dvmrp-rib {
 import-rib inet.2;
 export-rib inet.2;
 }
 }
}
```

```
 /* A comment here is dropped */
 }
 /* A comment here is dropped */
}
/* A comment here is dropped */
}
```

When you include comments in the configuration file directly, you can format comments in the following ways:

- Start the comment with a `/*` and end it with a `*/`. The comment text can be on a single line or can span multiple lines.
- Start the comment with a `#` and end it with a new line (carriage return).

**Related  
Documentation**

- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Example: Including Comments in a Junos OS Configuration by Using the CLI on page 494](#)

---

## Example: Including Comments in a Junos OS Configuration by Using the CLI

---

Adding comments to a Junos OS configuration makes the configuration file readable and more readily understood by users. Using the Junos OS CLI, you can include comments as you configure by using the **annotate** statement. In this example, comments are added by using the CLI for an already existing configuration:

- [Requirements on page 494](#)
- [Overview on page 495](#)
- [Configuration on page 495](#)

### Requirements

No special configuration beyond device initialization is required before configuring this example.

Before you add a comment, you must configure the following hierarchy on the router.

To quickly configure the *initial configuration* for this example, copy the following command, paste it into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste this command into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set protocols ospf area 0.0.0.0 interface so-0/0/0.0 hello-interval 5
```

Now, check that you have this hierarchy configured.

```
user@host# show protocols
ospf {
 area 0.0.0.0 {
 interface so-0/0/0 {
 hello-interval 5;
 }
 }
}
```

```
}
```

## Overview

When you add comments by using the CLI, you do so in configuration mode using the **annotate** statement. Each comment you add is associated with a statement at the current level. Each statement can have one single-line comment associated with it.

To configure the **annotate** statement, move to the level of the statement with which you want to associate a comment. To view the comments, go to the top of the configuration hierarchy and use the **show** command.

## Configuration

### CLI Quick Configuration

To quickly configure the *comments* for this example, copy the following commands, paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste the commands into the CLI, starting at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
edit protocols ospf
annotate area 0.0.0.0 "Backbone area configuration added June 15, 1998"
edit area 0.0.0.0
annotate interface so-0/0/0.0 "Interface from router sj1 to router sj2"
```

Notice that the commands are moving you down the hierarchy as you annotate different sections of the hierarchy.

### Including Comments in the CLI Configuration Mode

### Step-by-Step Procedure

This procedure assumes that you have already configured the initial configuration.

To add comments to a configuration:

1. Move to the first hierarchy level to which you need to add a comment.  

```
[edit]
user@host# edit protocols ospf
```
2. Add a comment to the **area** configuration statement by using the **annotate** statement.  

```
[edit protocols ospf]
user@host# annotate area 0.0.0.0 "Backbone area configuration added June 15, 1998"
```
3. Move down a level to the **interface** configuration statement.  

```
[edit protocols ospf]
user@host# edit area 0.0.0.0
```
4. Add a comment to interface so-0/0/0.0 by using the **annotate** statement.  

```
[edit protocols ospf area 0.0.0.0]
user@host# annotate interface so-0/0/0.0 "Interface from router sj1 to router sj2"
```

## Results

---

Move to the top of the hierarchy and use the **show** command to see the comments you added. The comments precede the statement they are associated with.

```
[edit]
user@host# show protocols
ospf {
 /* Backbone area configuration added June 15, 1998 */
 area 0.0.0.0 {
 /* Interface from router sj1 to router sj2 */
 interface so-0/0/0.0 {
 hello-interval 5;
 }
 }
}
```

After you have confirmed that the configuration is correct, enter the **commit** command.

**Related Documentation** • [Adding Comments in a Junos OS Configuration on page 492](#)

## Updating the configure private Configuration

---

When you are in configure private mode, you must work with a copy of the most recently committed shared configuration. If the global configuration changes, you can issue the **update** command to update your private candidate configuration. When you do this, your private candidate configuration contains a copy of the most recently committed configuration with your private changes merged in. For example:

```
[edit]
user@host# update
[edit]
user@host#
```



**NOTE:** Merge conflicts can occur when you issue the **update** command.

You can also issue the **rollback** command to discard your private candidate configuration changes and obtain the most recently committed configuration:

```
[edit]
user@host# rollback
[edit]
user@host#
```

**Related Documentation** • [Forms of the configure Command on page 465](#)



## Displaying the Current Junos OS Configuration

To display the current configuration for a device running Junos OS, use the **show** configuration mode command. This command displays the configuration at the current hierarchy level or at the specified level.

```
user@host# show <statement-path>
```

The configuration statements appear in a fixed order, interfaces appear alphabetically by type, and then in numerical order by slot number, PIC number, and port number. Note that when you configure the router, you can enter statements in any order.

You also can use the CLI operational mode **show configuration** command to display the last committed current configuration, which is the configuration currently running on the router:

```
user@host> show configuration
```

When you show a configuration, a timestamp at the top of the configuration indicates when the configuration was last changed:

```
Last commit: 2006-07-18 11:21:58 PDT by echen
version 8.3
```

If you have omitted a required statement at a particular hierarchy level, when you issue the **show** command in configuration mode, a message indicates which statement is missing. As long as a mandatory statement is missing, the CLI continues to display this message each time you issue a **show** command. For example:

```
[edit]
user@host# show
protocols {
 pim {
 interface so-0/0/0 {
 priority 4;
 version 2;
 # Warning: missing mandatory statement(s): 'mode'
 }
 }
}
```

When you issue the **show configuration** command with the **| display set** pipe option to view the configuration as **set** commands, those portions of the configuration that you do not have permissions to view are substituted with the text **ACCESS-DENIED**.

Unsupported statements included in the CLI configuration are displayed with the “unsupported” text in the configuration. For example, if a statement is configured on an unsupported platform, the CLI displays a message that the statement is ignored in the configuration because it is configured on an unsupported platform. When you issue the **show** command with the **| display xml** option, you can see the **unsupported="unsupported"** attribute for configuration that is unsupported.

The “unsupported” attribute included in text configuration or XML configuration is provided to scripts when the **unsupported="unsupported"** attribute is included in the **<get-configuration>** RPC call.

**Related  
Documentation**

- [Example: Displaying the Current Junos OS Configuration on page 498](#)
- [Displaying set Commands from the Junos OS Configuration on page 501](#)

---

## Example: Displaying the Current Junos OS Configuration

The following example shows how you can display the current Junos configuration.

**Set a** configuration:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
```

**To display the current configuration:**

```
[edit]
user@host# show
protocols {
 ospf {
 area 0.0.0.0 {
 interface so-0/0/0 {
 hello-interval 5;
 }
 }
 }
}
```

Display a particular hierarchy in the configuration:

```
[edit]
user@host# show protocols ospf area 0.0.0.0
interface so-0/0/0 {
 hello-interval 5;
}
```

Move down a level and display the configuration at that level:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# show
interface so-0/0/0 {
 hello-interval 5;
}
```

**Set and commit a configuration:**

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface so-0/0/0 hello-interval 5
[edit]
user@host# commit
commit complete
```

```
[edit]
user@host# quit
exiting configuration mode
```

Display the last committed configuration:

```
user@host> show configuration
Last commit: 2006-08-10 11:21:58 PDT by user
version 8.3
protocols {
 ospf {
 area 0.0.0.0 {
 interface so-0/0/0 {
 hello-interval 5;
 }
 }
 }
}
```

**Related Documentation**

- [Displaying the Current Junos OS Configuration on page 497](#)

## Displaying Additional Information About the Junos OS Configuration

In configuration mode only, to display additional information about the configuration, use the **display detail** command after the pipe ( | ) in conjunction with a **show** command. The additional information includes the help string that explains each configuration statement and the permission bits required to add and modify the configuration statement.

```
user@host# show <hierarchy-level> | display detail
```

For example:

```
[edit]
user@host# show | display detail
##
version: Software version information
require: system
##
version "3.4R1 [tlim]";
system {
 ##
 ## host-name: Host name for this router
 ## match: ^[:alnum:]._-]+$
 ## require: system
 ##
}
host-name router-name;
##
domain-name: Domain name for this router
match: ^[:alnum:]._-]+$
require: system
##
domain-name isp.net;
##
```

```
backup-router: Address of router to use while booting
##
backup-router 192.168.100.1;
root-authentication {
 ##
 ## encrypted-password: Encrypted password string
 ##
 encrypted-password "$ABC123"; # SECRET-DATA
}
##
name-server: DNS name servers
require: system
##
name-server {
 ##
 ## name-server: DNS name server address
 ##
 208.197.1.0;
}
login {
 ##
 ## class: User name (login)
 ## match: ^[:alnum:._-]+$
 ##
 class super-user {
 ##
 ## permissions: Set of permitted operation categories
 ##
 permissions all;
 }
 ...
 ##
 ## services: System services
 ## require: system
 ##
 services {
 ## services: Service name
 ##
 ftp;
 ##
 ## services: Service name
 ##
 telnet;
 ##
 }
 syslog {
 ##
 ## file-name: File to record logging data
 ##
 file messages {
 ##
 ## Facility type
 ## Level name
 ##
 any notice;
 ##
 }
 }
}
```

```

 ## Facility type
 ## Level name
 ##
 authorization info;
 }
}
chassis {
 alarm {
 sonet {
 ##
 ## lol: Loss of light
 ## alias: loss-of-light
 ##
 lol red;
 }
 }
}
interfaces {
 ##
 ## Interface name
 ##
 at-2/1/1 {
 atm-options {
 ##
 ## vpi: Virtual path index
 ## range: 0 .. 255
 ## maximum-vcs: Maximum number of virtual circuits on this VP
 ##
 vpi 0 maximum-vcs 512;
 }
 ##
 ## unit: Logical unit number
 ## range: 0 .. 16384
 ##
 unit 0 {
 ##
 ## vci: ATM point-to-point virtual circuit identifier ([vpi.]vci)
 ##
 vci 0.128;
 }
 }
}
...

```

#### Related Documentation

- [Displaying set Commands from the Junos OS Configuration on page 501](#)

## Displaying set Commands from the Junos OS Configuration

In configuration mode, you can display the configuration as a series of configuration mode commands required to re-create the configuration. This is useful if you are not familiar

with how to use configuration mode commands or if you want to cut, paste, and edit the displayed configuration.

To display the configuration as a series of configuration mode commands, which are required to re-create the configuration from the top level of the hierarchy as **set** commands, issue the **show** configuration mode command with the **display set** option:

```
user@host# show | display set
```

This topic contains the following examples:

- [Example: Displaying set Commands from the Configuration on page 502](#)
- [Example: Displaying Required set Commands at the Current Hierarchy Level on page 502](#)
- [Example: Displaying set Commands with the match Option on page 503](#)

### Example: Displaying set Commands from the Configuration

Display the **set** commands from the configuration at the **[edit interfaces]** hierarchy level:

```
[edit interfaces fe-0/0/0]
user@host# show
unit 0 {
 family inet {
 address 192.107.1.230/24;
 }
 family iso;
 family mpls;
}
inactive: unit 1 {
 family inet {
 address 10.0.0.1/8;
 }
}
user@host# show | display set
set interfaces fe-0/0/0 unit 0 family inet address 192.107.1.230/24
set interfaces fe-0/0/0 unit 0 family iso
set interfaces fe-0/0/0 unit 0 family mpls
set interfaces fe-0/0/0 unit 1 family inet address 10.0.0.1/8
deactivate interfaces fe-0/0/0 unit 1
```

To display the configuration as a series of configuration mode commands required to re-create the configuration from the current hierarchy level, issue the **show** configuration mode command with the **display set relative** option:

```
user@host# show | display set relative
```

### Example: Displaying Required set Commands at the Current Hierarchy Level

Display the configuration as a series of configuration mode commands required to re-create the configuration from the current hierarchy level:

```
[edit interfaces fe-0/0/0]
user@host# show
unit 0 {
 family inet {
```

```

 address 192.107.1.230/24;
 }
 family iso;
 family mpls;
}
inactive: unit 1 {
 family inet {
 address 10.0.0.1/8;
 }
}
user@host# show | display set relative
set unit 0 family inet address 192.107.1.230/24
set unit 0 family iso
set unit 0 family mpls
set unit 1 family inet address 10.0.0.1/8
deactivate unit 1

```

To display the configuration as **set** commands and search for text matching a regular expression by filtering output, specify the **match** option after the pipe ( | ):

```
user@host# show | display set | match regular-expression
```

### Example: Displaying set Commands with the match Option

Display IP addresses associated with an interface:

```

xe-2/3/0 {
 unit 0 {
 family inet {
 address 192.107.9.106/30;
 }
 }
}
so-5/1/0 {
 unit 0 {
 family inet {
 address 192.107.9.15/32 {
 destination 192.107.9.192;
 }
 }
 }
}
lo0 {
 unit 0 {
 family inet {
 address 127.0.0.1/32;
 }
 }
}
user@host# show interfaces | display set | match address
set interfaces xe-2/3/0 unit 0 family inet address 192.168.9.106/30
set interfaces so-5/1/0 unit 0 family inet address 192.168.9.15/32 destination 192.168.9.192
set interfaces lo0 unit 0 family inet address 127.0.0.1/32

```

**Related Documentation**

- [Displaying the Current Junos OS Configuration on page 497](#)

## Displaying Users Currently Editing the Junos OS Configuration

---

To display the users currently editing the configuration, use the **status** configuration mode command:

```
user@host# status
Users currently editing the configuration:
rchen terminal p0 (pid 55691) on since 2006-03-01 13:17:25 PST
[edit interfaces]
```

The system displays who is editing the configuration (**rchen**), where the user is logged in (**terminal p0**), the date and time the user logged in (**2006-03-01 13:17:25 PST**), and what level of the hierarchy the user is editing (**[edit interfaces]**).

If you issue the **status** configuration mode command and a user has scheduled a candidate configuration to become active for a future time, the system displays who scheduled the commit (**root**), where the user is logged in (**terminal d0**), the date and time the user logged in (**2002-10-31 14:55:15 PST**), and that a commit is pending (**commit at**).

```
[edit]
user@host# status
Users currently editing the configuration:
root terminal d0 (pid 767) on since 2002-10-31 14:55:15 PST, idle 00:03:09
commit at
```

For information about how to schedule a commit, see [“Scheduling a Junos OS Commit Operation” on page 513](#).

If you issue the **status** configuration mode command and a user is editing the configuration in configure exclusive mode, the system displays who is editing the configuration (**root**), where the user is logged in (**terminal d0**), the date and time the user logged in (**2002-11-01 13:05:11 PST**), and that a user is editing the configuration in configure exclusive mode (**exclusive [edit]**).

```
[edit]
user@host# status
Users currently editing the configuration:
root terminal d0 (pid 2088) on since 2002-11-01 13:05:11 PST
exclusive [edit]
```

### Related Documentation

- [Forms of the configure Command on page 465](#)
- [Using the configure exclusive Command on page 467](#)

## Verifying a Junos OS Configuration

---

To verify that the syntax of a Junos configuration is correct, use the configuration mode **commit check** command:

```
[edit]
user@host# commit check
configuration check succeeds
[edit]
```



user@host#

If the **commit check** command finds an error, a message indicates the location of the error.

**Related  
Documentation**

- [Adding Junos OS Configuration Statements and Identifiers on page 469](#)
- [Committing a Junos OS Configuration on page 508](#)



# Committing a Junos OS Configuration

- [Junos OS Commit Model for Router or Switch Configuration on page 507](#)
- [Committing a Junos OS Configuration on page 508](#)
- [Committing a Junos OS Configuration and Exiting Configuration Mode on page 510](#)
- [Commit Operation When Multiple Users Configure the Software on page 511](#)
- [Activating a Junos OS Configuration but Requiring Confirmation on page 512](#)
- [Scheduling a Junos OS Commit Operation on page 513](#)
- [Monitoring the Junos OS Commit Process on page 514](#)
- [Adding a Comment to Describe the Committed Configuration on page 515](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 516](#)
- [Junos OS Batch Commits Overview on page 516](#)
- [Example: Configuring Batch Commit Server Properties on page 517](#)

## Junos OS Commit Model for Router or Switch Configuration

---

The router or switch configuration is saved using a commit model—a candidate configuration is modified as desired and then committed to the system. When a configuration is committed, the router or switch checks the configuration for syntax errors, and if no errors are found, the configuration is saved as **juniper.conf.gz** and activated. The formerly active configuration file is saved as the first rollback configuration file (**juniper.conf.1.gz**), and any other rollback configuration files are incremented by 1. For example, **juniper.conf.1.gz** is incremented to **juniper.conf.2.gz**, making it the second rollback configuration file. The router or switch can have a maximum of 49 rollback configurations (numbered 1 through 49) saved on the system.

On the router or switch, the active configuration file and the first three rollback files (**juniper.conf.gz.1**, **juniper.conf.gz.2**, **juniper.conf.gz.3**) are located in the **/config** directory. If the file **rescue.conf.gz** is saved on the system, this file should also be saved in the **/config** directory. The factory default files are located in the **/etc/config** directory.

There are two mechanisms used to propagate the configurations between Routing Engines within a router or switch:

- **Synchronization**—Propagates a configuration from one Routing Engine to a second Routing Engine within the same router or switch chassis.



**NOTE:** The QFX3500 switch has only one Routing Engine.

To synchronize configurations, use the **commit synchronize** CLI command. If one of the Routing Engines is locked, the synchronization fails. If synchronization fails because of a locked configuration file, you can use the **commit synchronize force** command. This command overrides the lock and synchronizes the configuration files.

- **Distribution**—Propagates a configuration across the routing plane on a multichassis router or switch. Distribution occurs automatically. There is no user command available to control the distribution process. If a configuration is locked during a distribution of a configuration, the locked configuration does not receive the distributed configuration file, so the synchronization fails. You need to clear the lock before the configuration and resynchronize the routing planes.



**NOTE:** When you use the **commit synchronize force** CLI command on a multichassis platform, the forced synchronization of the configuration files does not affect the distribution of the configuration file across the routing plane. If a configuration file is locked on a router or switch remote from the router or switch where the command was issued, the synchronization fails on the remote router or switch. You need to clear the lock and reissue the **synchronize** command.

**Related  
Documentation**

- *Configuring Junos OS for the First Time on a Router or Switch with a Single Routing Engine*
- [commit on page 662](#)

---

## Committing a Junos OS Configuration

---

To save Junos OS configuration changes to the configuration database and to activate the configuration on the router, use the **commit** configuration mode command. You can issue the **commit** command from any hierarchy level:

```
[edit]
user@host# commit
commit complete
[edit]
user@host#
```

When you enter the **commit** command, the configuration is first checked for syntax errors (**commit check**). Then, if the syntax is correct, the configuration is activated and becomes the current, operational router configuration.

You can issue the **commit** command from any hierarchy level.

A configuration commit can fail for any of the following reasons:

- The configuration includes incorrect syntax, which causes the commit check to fail.

- The candidate configuration that you are trying to commit is larger than 700 MB.
- The configuration is locked by a user who entered the **configure exclusive** command.

If the configuration contains syntax errors, a message indicates the location of the error, and the configuration is not activated. The error message has the following format:

```
[edit edit-path]
'offending-statement;'
error-message
```

For example:

```
[edit firewall filter login-allowed term allowed from]
'icmp-type [echo-request echo-reply];'
keyword 'echo-reply' unrecognized
```

You must correct the error before recommitting the configuration. To return quickly to the hierarchy level where the error is located, copy the path from the first line of the error and paste it at the configuration mode prompt at the **[edit]** hierarchy level.

The uncommitted, candidate configuration file is `/var/run/db/juniper.db`. It is limited to 700 MB. If the commit fails with a message **configuration database size limit exceeded**, view the file size from configuration mode by entering the command **run file list /var/run/db detail**. You can simplify the configuration and reduce the file size by creating configuration groups with wildcards or defining less specific match policies in your firewall filters.



**NOTE:** CLI commit-time warnings displayed for configuration changes at the **[edit interfaces]** hierarchy level are removed and are logged as system log messages.

This is also applicable to VRRP configuration at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* family (*inet* | *inet6*) address *address*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (*inet* | *inet6*) address *address*]**

When you commit a configuration, you commit the entire configuration in its current form. If more than one user is modifying the configuration, committing it saves and activates the changes of all the users.

**NOTE:**

- If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

load merge  
load replace  
load override  
load update

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

- We do not recommend performing a commit operation on the backup Routing Engine when graceful Routing Engine switchover is enabled on the router.



**NOTE:** If you configure the same IP address for a management interface or internal interface such as fxp0 and an external physical interface such as ge-0/0/1, when graceful Routing Engine switchover (GRES) is enabled, the CLI displays an appropriate commit error message that identical addresses have been found on the private and public interfaces. In such cases, you must assign unique IP addresses for the two interfaces that have duplicate addresses.

The management Ethernet interface used for the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers, is em0. Junos OS automatically creates the router's management Ethernet interface, em0.

**Related Documentation**

- [Committing a Junos OS Configuration and Exiting Configuration Mode on page 510](#)
- [Activating a Junos OS Configuration but Requiring Confirmation on page 512](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 516](#)
- [Forms of the configure Command on page 465](#)

## Committing a Junos OS Configuration and Exiting Configuration Mode

To save Junos OS configuration changes, activate the configuration on the device and exit configuration mode, using the **commit and-quit** configuration mode command. This command succeeds only if the configuration contains no errors.

```
[edit]
user@host# commit and-quit
commit complete
```

```

exiting configuration mode
user@host>

```



**NOTE:** We do not recommend performing a commit operation on the backup Routing Engine when graceful Routing Engine switchover is enabled on the router.

**Related  
Documentation**

- [Activating a Junos OS Configuration but Requiring Confirmation on page 512](#)

## Commit Operation When Multiple Users Configure the Software

Up to 32 users can be in configuration mode simultaneously, and they all can be making changes to the configuration. All changes made by all users are visible to everyone editing the configuration—the changes become visible as soon as the user presses the Enter key at the end of a command that changes the configuration, such as **set**, **edit**, or **delete**.

When any of the users editing the configuration issues a **commit** command, all changes made by all users are checked and activated.

If you enter configuration mode with the **configure private** command, each user has a private candidate configuration to edit somewhat independently of other users. When you commit the configuration, only your own changes get committed. To synchronize your copy of the configuration after other users have committed changes, you can run the **update** command in configuration mode. A commit operation also updates all of the private candidate configurations. For example, suppose user X and user Y are both in **configure private** mode, and user X commits a configuration change. When user Y performs a subsequent commit operation and then views the new configuration, the new configuration seen by user Y includes the changes made by user X.

If you enter configuration mode with the **configure exclusive** command, you lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. Other users can enter and exit configuration mode, but they cannot commit the configuration. This is true even if the other users entered configuration mode before you enter the **configure exclusive** command. For example, suppose user X is already in the **configure private** or **configure** mode. Then suppose user Y enters the **configure exclusive** mode. User X cannot commit any changes to the configuration, even if those changes were entered before user Y logged in. If user Y exits **configure exclusive** mode, user X can then commit the changes made in **configure private** or **configure** mode.

**Related  
Documentation**

- [Committing a Junos OS Configuration on page 508](#)
- [Forms of the configure Command on page 465](#)
- [Displaying Users Currently Editing the Junos OS Configuration on page 504](#)

## Activating a Junos OS Configuration but Requiring Confirmation

---

When you commit the current candidate configuration, you can require an explicit confirmation for the commit to become permanent. This is useful if you want to verify that a configuration change works correctly and does not prevent access to the router. If the change prevents access or causes other errors, the router automatically returns to the previous configuration and restores access after the rollback confirmation timeout passes. This feature is called automatic rollback.

To commit the current candidate configuration but require an explicit confirmation for the commit to become permanent, use the **commit confirmed** configuration mode command:

```
[edit]
user@host# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless confirmed
commit complete
#commit confirmed will be rolled back in 10 minutes
[edit]
user@host#
```

Once you have verified that the change works correctly, you can keep the new configuration active by entering a **commit** or **commit check** command within 10 minutes of the **commit confirmed** command. For example:

```
[edit]
user@host# commit check
commit confirmed will be automatically rolled back in 10 minutes unless confirmed
commit complete
#commit confirmed will be rolled back in 10 minutes
[edit]
user@host#
```

If the commit is not confirmed within a certain time (10 minutes by default), Junos OS automatically rolls back to the previous configuration and a broadcast message is sent to all logged-in users.

To show when a rollback is scheduled after a **commit confirmed** command, enter the **show system commit** command. For example:

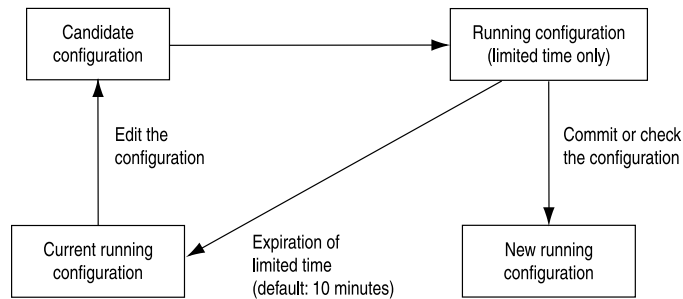
```
user@host>show system commit
0 2005-01-05 15:00:37 PST by root via cli commit confirmed, rollback in 3mins
```

Like the **commit** command, the **commit confirmed** command verifies the configuration syntax and reports any errors. If there are no errors, the configuration is activated and begins running on the router.

Figure 14 illustrates how the **commit confirmed** command works.



Figure 14: Confirm a Configuration



To change the amount of time before you have to confirm the new configuration, specify the number of minutes when you issue the command:

```

[edit]
user@host# commit confirmed minutes
commit complete
[edit]
user@host#

```

In Junos OS Release 11.4 and later, you can also use the **commit confirmed** command in the **[edit private]** configuration mode.

#### Related Documentation

- [Scheduling a Junos OS Commit Operation on page 513](#)
- [Committing a Junos OS Configuration on page 508](#)

## Scheduling a Junos OS Commit Operation

You can schedule when you want your candidate configuration to become active. To save Junos OS configuration changes and activate the configuration on the router at a future time or upon reboot, use the **commit at** configuration mode command, specifying **reboot** or a future time at the **[edit]** hierarchy level:

```

[edit]
user@host # commit at string

```

Where **string** is **reboot** or the future time to activate the configuration changes. You can specify time in two formats:

- A time value in the form **hh:mm[:ss]** (hours, minutes, and optionally seconds)—Commit the configuration at the specified time, which must be in the future but before 11:59:59 PM on the day the **commit at** configuration mode command is issued. Use 24-hour time for the **hh** value; for example, **04:30:00** is 4:30:00 AM, and **20:00** is 8:00 PM. The time is interpreted with respect to the clock and time zone settings on the router.
- A date and time value in the form **yyyy-mm-dd hh:mm[:ss]** (year, month, date, hours, minutes, and, optionally, seconds)—Commit the configuration at the specified day and time, which must be after the **commit at** command is issued. Use 24-hour time for the **hh** value. For example, **2003-08-21 12:30:00** is 12:30 PM on August 21, 2003. The time is interpreted with respect to the clock and time zone settings on the router.

Enclose the **string** value in quotation marks (" "). For example, **commit at "18:00:00"**. For date and time, include both values in the same set of quotation marks. For example, **commit at "2005-03-10 14:00:00"**.

A commit check is performed immediately when you issue the **commit at** configuration mode command. If the result of the check is successful, then the current user is logged out of configuration mode, and the configuration data is left in a read-only state. No other commit can be performed until the scheduled commit is completed.



**NOTE:** If Junos OS fails before the configuration changes become active, all configuration changes are lost.

You cannot enter the **commit at** configuration command after you issue the **request system reboot** command.

You cannot enter the **request system reboot** command once you schedule a commit operation for a specific time in the future.

You cannot commit a configuration when a scheduled commit is pending. For information about how to cancel a scheduled configuration by means of the **clear** command, see the [CLI Explorer](#).



**NOTE:** We do not recommend performing a commit operation on the backup Routing Engine when graceful Routing Engine switchover is enabled on the router.

**Related Documentation**

- [Committing a Junos OS Configuration on page 508](#)
- [Monitoring the Junos OS Commit Process on page 514](#)

---

## Monitoring the Junos OS Commit Process

To monitor the Junos commit process, use the **display detail** command after the pipe with the **commit** command:

```
user@host# commit | display detail
```

For example:

```
[edit]
user@host# commit | display detail
2003-09-22 15:39:39 PDT: exporting juniper.conf
2003-09-22 15:39:39 PDT: setup foreign files
2003-09-22 15:39:39 PDT: propagating foreign files
2003-09-22 15:39:39 PDT: complete foreign files
2003-09-22 15:39:40 PDT: copying configuration to juniper.data+
2003-09-22 15:39:40 PDT: dropping unchanged foreign files
2003-09-22 15:39:40 PDT: daemons checking new configuration
2003-09-22 15:39:41 PDT: commit wrapup...
```

```

2003-09-22 15:39:42 PDT: activating '/var/etc/ntp.conf'
2003-09-22 15:39:42 PDT: activating '/var/etc/kmd.conf'
2003-09-22 15:39:42 PDT: activating '/var/db/juniper.data'
2003-09-22 15:39:42 PDT: notifying daemons of new configuration
2003-09-22 15:39:42 PDT: signaling 'Firewall daemon', pid 24567, signal 1,
status 0
2003-09-22 15:39:42 PDT: signaling 'Interface daemon', pid 24568, signal 1,
status 0
2003-09-22 15:39:43 PDT: signaling 'Routing protocol daemon', pid 25679,
signal 1, status 0
2003-09-22 15:39:43 PDT: signaling 'MIB2 daemon', pid 24549, signal 1,
status 0
2003-09-22 15:39:43 PDT: signaling 'NTP daemon', pid 37863, signal 1, status 0
2003-09-22 15:39:43 PDT: signaling 'Sonet APS daemon', pid 24551, signal 1,
status 0
2003-09-22 15:39:43 PDT: signaling 'VRRP daemon', pid 24552, signal 1,
status 0
2003-09-22 15:39:43 PDT: signaling 'PFE daemon', pid 2316, signal 1, status 0
2003-09-22 15:39:43 PDT: signaling 'Traffic sampling control daemon', pid 24553
signal 1, status 0
2003-09-22 15:39:43 PDT: signaling 'IPsec Key Management daemon', pid
24556, signal 1, status 0
2003-09-22 15:39:43 PDT: signaling 'Forwarding UDP daemon', pid 2320,
signal 1, status 0
commit complete

```

**Related  
Documentation**

- [Committing a Junos OS Configuration on page 508](#)
- [Adding a Comment to Describe the Committed Configuration on page 515](#)

## Adding a Comment to Describe the Committed Configuration

You can include a comment that describes changes to the committed configuration. To do so, include the `commit comment` statement. The comment can be as long as 512 bytes and you must type it on a single line.

```

[edit]
user@host# commit comment comment-string

```

*comment-string* is the text of the comment.



**NOTE:** You cannot include a comment with the `commit check` command.

To add a comment to the `commit` command, include the `comment` statement after the `commit` command:

```

[edit]
user@host# commit comment "add user joe"
commit complete
[edit]
user@host#

```

To add a comment to the **commit confirmed** command, include the **comment** statement after the **commit confirmed** command:

```
[edit]
user@host# commit confirmed comment "add customer to port 27"
commit confirmed will be automatically rolled back in 10 minutes unless confirmed
commit complete
[edit]
user@host#
```

To view these commit comments, issue the **show system commit** operational mode command.

In Junos OS Release 11.4 and later, you can also use the **commit confirmed** command in the **[edit private]** configuration mode.

- Related Documentation**
- [Committing a Junos OS Configuration on page 508](#)
  - [Backing Up the Committed Configuration on the Alternate Boot Drive on page 516](#)

---

## Backing Up the Committed Configuration on the Alternate Boot Drive

---

After you commit the configuration and are satisfied that it is running successfully, you should issue the **request system snapshot** command to back up the new software onto the **/altconfig** file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The **request system snapshot** command backs up the root file system to **/altroot**, and **/config** to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard disk (if available).



**NOTE:** For more information about backing up the file system on an ACX Series Universal Access Router, see *Understanding System Snapshot on an ACX Series Router*.

After you issue the **request system snapshot** command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

- Related Documentation**
- [Committing a Junos OS Configuration on page 508](#)

---

## Junos OS Batch Commits Overview

---

Junos OS provides a batch commit feature that aggregates or merges multiple configuration edits from different CLI sessions or users and adds them to a batch commit queue. A batch commit server running on the device takes one or more jobs from the batch commit queue, applies the configuration changes to the shared configuration database, and then commits the configuration changes in a single commit operation.

Batches are prioritized by the commit server based on priority of the batch specified by the user or the time when the batch job is added. When one batch commit is complete, the next set of configuration changes are aggregated and loaded into the batch queue for the next session of the batch commit operation. Batches are created until there are no commit entries left in the queue directory.

When compared to the regular commit operation where all commits are independently committed sequentially, batch commits save time and system resources by committing multiple small configuration edits in a single commit operation.

Batch commits are performed from the **[edit batch]** configuration mode. The commit server properties can be configured at the **[edit system commit server]** hierarchy level.

## Aggregation and Error Handling

When there is a load-time error in one of the aggregated jobs, the commit job that encounters the error is discarded and the remaining jobs are aggregated and committed.

For example, if there are five commit jobs (**commit-1**, **commit-2**, **commit-3**, **commit-4**, and **commit-5**) being aggregated, and **commit-3** encounters an error while loading, **commit-3** is discarded and **commit-1**, **commit-2**, **commit-4**, and **commit-5** are aggregated and committed.

If there is an error during the commit operation when two or more jobs are aggregated and committed, the aggregation is discarded and each of those jobs is committed individually like a regular commit operation.

For example, if there are five commit jobs (**commit-1**, **commit-2**, **commit-3**, **commit-4**, and **commit-5**) that are aggregated and if there is a commit error caused because of **commit-3**, the aggregation is discarded, **commit-1**, **commit-2**, **commit-3**, **commit-4**, and **commit-5** are committed individually, and the CLI reports a commit error for **commit-3**.

### Related Documentation

- [Example: Configuring Batch Commit Server Properties on page 517](#)

## Example: Configuring Batch Commit Server Properties

This example shows how to configure batch commit server properties to manage batch commit operations.

- [Requirements on page 517](#)
- [Overview on page 518](#)
- [Configuration on page 518](#)
- [Verification on page 520](#)

## Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router
- Junos OS Release 12.1 or later running on the device

## Overview

You can control how the batch commit queue is handled by the commit server by configuring the server properties at the **[edit system commit server]** hierarchy level. This enables you to control how many commit jobs are aggregated or merged into a single batch commit, the maximum number of jobs that can be added to the queue, days to keep batch commit error logs, interval between two batch commits, and tracing operations for batch commit operations.

## Configuration

### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level. You can configure the commit server properties from either the regular **[edit]** mode or the **[edit batch]** mode.

**Device R0**

```
set system commit server maximum-aggregate-pool 4
set system commit server maximum-entries 500
set system commit server commit-interval 5
set system commit server days-to-keep-error-logs 30
set system commit server traceoptions file commitd_nov
set system commit server traceoptions flag all
```

### Configuring the Commit Server Properties

#### Step-by-Step Procedure

1. (Optional) Configure the number of commit transactions to aggregate or merge in a single commit operation.

The default value for **maximum-aggregate-pool** is 5.



**NOTE:** Setting **maximum-aggregate-pool** to 1 commits each of the jobs individually.

In this example, the number of commit transactions is set to 4 indicating that four different commit jobs are aggregated into a single commit before the commit operation is initiated.

```
[edit system commit server]
user@R0# set maximum-aggregate-pool 4
```

2. (Optional) Configure the maximum number of jobs allowed in a batch.

This limits the number of commits jobs that are added to the queue.

```
[edit system commit server]
user@R0# set maximum-entries 500
```



**NOTE:** If you set **maximum-entries** to 1, the commit server cannot add more than one job to the queue, and the CLI displays an appropriate message when you try to commit more than one job.

3. (Optional) Configure the time (in seconds) to wait before starting the next batch commit operation.

```
[edit system commit server]
user@R0# set commit-interval 5
```

4. (Optional) Configure the number of days to keep error logs.

The default value is 30 days.

```
[edit system commit server]
user@R0# set days-to-keep-error-logs 30
```

5. (Optional) Configure tracing operations to log batch commit events.

In this example, the filename for logging batch commit events is **commitd\_nov**, and all traceoption flags are set.

```
[edit system commit server]
user@R0# set traceoptions commitd_nov
user@R0# set traceoptions flag all
```

**Results** From configuration mode, confirm your configuration by entering the **show system commit server** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R0# show system commit server
maximum-aggregate-pool 4;
maximum-entries 500;
commit-interval 5;
days-to-keep-error-logs 30;
traceoptions {
 file commitd_nov;
 flag all;
}
```

### Committing the Configuration from Batch Configuration Mode

**Step-by-Step Procedure** To commit the configuration from the **[edit batch]** mode, do one of the following:

- Log in to the device and enter **commit**.

```
[edit batch]
user@R0# commit
Added to commit queue request-id: 1000
```

- To assign a higher priority to a batch commit job, issue the **commit** command with the **priority** option.

```
[edit batch]
user@R0# commit priority
Added to commit queue request-id: 1001
```

- To commit a configuration without aggregating the configuration changes with other commit jobs in the queue, issue the **commit** command with the **atomic** option.

```
[edit batch]
user@R0# commit atomic
Added to commit queue request-id: 1002
```

- To commit a configuration without aggregating the configuration changes with other commit jobs in the queue, and issuing a higher priority to the commit job, issue the **commit** command with the **atomic priority** option.

[edit batch]

user@R0# **commit atomic priority**

Added to commit queue request-id: 1003

## Verification

Confirm that the configuration is working properly.

- [Checking the Batch Commit Server Status on page 520](#)
- [Checking the Batch Commit Status on page 520](#)
- [Viewing the Patch Files in a Batch Commit Job on page 521](#)
- [Viewing the Trace Files for Batch Commit Operations on page 523](#)

---

### Checking the Batch Commit Server Status

**Purpose** Check the status of the batch commit server.

**Action** user@R0> **show system commit server**  
Commit server status : Not running

By default, the status of the commit server is **Not running**. The commit server starts running only when a batch commit job is added to the queue.

When a batch commit job is added to the queue, the status of the commit server changes to **Running**.

user@R0> **show system commit server**

Commit server status : Running  
Jobs in process:  
1003 1004 1005

**Meaning** The **Jobs in process** field lists the commit IDs of jobs that are in process.

---

### Checking the Batch Commit Status

**Purpose** Check the commit server queue for the status of the batch commits.



**Action** user@R0> show system commit server queue

```
Pending commits:
 Id: 1005
 Last Modified: Tue Nov 1 23:56:43 2011

Completed commits:
 Id: 1000
 Last Modified: Tue Nov 1 22:46:43 2011
 Status: Successfully committed 1000

 Id: 1002
 Last Modified: Tue Nov 1 22:50:35 2011
 Status: Successfully committed 1002

 Id: 1004
 Last Modified: Tue Nov 1 22:51:48 2011
 Status: Successfully committed 1004

 Id: 1007
 Last Modified: Wed Nov 2 01:08:04 2011
 Status: Successfully committed 1007

 Id: 1009
 Last Modified: Wed Nov 2 01:16:45 2011
 Status: Successfully committed 1009

 Id: 1010
 Last Modified: Wed Nov 2 01:19:25 2011
 Status: Successfully committed 1010

 Id: 1011
 Last Modified: Wed Nov 2 01:28:16 2011
 Status: Successfully committed 1011

Error commits:
 Id: 1008
 Last Modified: Wed Nov 2 01:08:18 2011
 Status: Error while committing 1008
```

**Meaning** **Pending commits** displays commit jobs that are added to the commit queue but are not committed yet. **Completed commits** displays the list of commit jobs that are successful. **Error commits** are commits that failed because of an error.

### Viewing the Patch Files in a Batch Commit Job

**Purpose** View the timestamps, patch files, and the status of each of the commit jobs. Patch files show the configuration changes that occur in each commit operation that is added to the batch commit queue.

**Action** 1. Issue the **show system commit server queue patch** command to view the patches for all commit operations.

```
user@R0> show system commit server queue patch
Pending commits:
 none
```

## Completed commits:

```
Id: 1000
Last Modified: Tue Nov 1 22:46:43 2011
Status: Successfully committed 1000
```

## Patch:

```
[edit groups]
 re1 { ... }
+ GRP-DHCP-POOL-NOACCESS {
+ access {
+ address-assignment {
+ pool <*> {
+ family inet {
+ dhcp-attributes {
+ maximum-lease-time 300;
+ grace-period 300;
+ domain-name verizon.net;
+ name-server {
+ 4.4.4.1;
+ 4.4.4.2;
+ }
+ }
+ }
+ }
+ }
+ }
+ }
```

```
Id: 1002
Last Modified: Tue Nov 1 22:50:35 2011
Status: Successfully committed 1002
```

## Patch:

```
[edit]
+ snmp {
+ community abc;
+ }
```

```
Id: 1010
Last Modified: Wed Nov 2 01:19:25 2011
Status: Successfully committed 1010
```

## Patch:

```
[edit system syslog]
 file test { ... }
+ file j {
+ any any;
+ }
```

## Error commits:

```
Id: 1008
Last Modified: Wed Nov 2 01:08:18 2011
Status: Error while committing 1008
```

## Patch:

```
[edit system]
+ radius-server {
+ 10.1.1.1 port 222;
+ }
```

The output shows the changes in configuration for each commit job ID.

- To view the patch for a specific commit job ID, issue the **show system commit server queue patch id <id-number>** command.

```
user@R0> show system commit server queue patch id 1000
```

```
Completed commits:
```

```
Id: 1000
```

```
Last Modified: Tue Nov 1 22:46:43 2011
```

```
Status: Successfully committed 1000
```

```
Patch:
```

```
[edit system]
```

```
+ radius-server {
```

```
+ 192.168.69.162 secret teH.bTc/RVbPM;
```

```
+ 192.168.64.10 secret teH.bTc/RVbPM;
```

```
+ 192.168.60.52 secret teH.bTc/RVbPM;
```

```
+ 192.168.60.55 secret teH.bTc/RVbPM;
```

```
+ 192.168.4.240 secret teH.bTc/RVbPM;
```

```
+ }
```

**Meaning** The output shows the patch created for a commit job. The + or - sign indicates the changes in the configuration for a specific commit job.

### Viewing the Trace Files for Batch Commit Operations

**Purpose** View the trace files for batch commit operations. You can use the trace files for troubleshooting purposes.

- Action**
- Issue the **file show /var/log/<filename>** command to view all entries in the log file.

```
user@R0> file show /var/log/commitd_nov
```

The output shows commit server event logs and other logs for batch commits.

```
Nov 1 22:46:43 Successfully committed 1000
```

```
Nov 1 22:46:43 pausing after commit for 0 seconds
```

```
...
```

```
Nov 1 22:46:43 Done working on queue
```

```
...
```

```
Nov 1 22:47:17 maximum-aggregate-pool = 5
```

```
Nov 1 22:47:17 maximum-entries= 0
```

```
Nov 1 22:47:17 asynchronous-prompt = no
```

```
Nov 1 22:47:17 commit-interval = 0
```

```
Nov 1 22:47:17 days-to-keep-error-logs = -1
```

```
...
```

```
Nov 1 22:47:17 Added to commit queue request-id: 1001
```

```
Nov 1 22:47:17 Commit server status=running
```

```
Nov 1 22:47:17 No need to pause
```

```
...
```

```
Nov 1 22:47:18 Error while committing 1001
```

```
Nov 1 22:47:18 doing rollback
```

```
...
```

- To view log entries only for successful batch commit operations, issue the **file show /var/log/<filename>** command with the **| match committed** pipe option.

```
user@R0> file show /var/log/commitd_nov | match committed
```

The output shows batch commit job IDs for successful commit operations.

```
Nov 1 22:46:43 Successfully committed 1000
Nov 1 22:50:35 Successfully committed 1002
Nov 1 22:51:48 Successfully committed 1004
Nov 2 01:08:04 Successfully committed 1007
Nov 2 01:16:45 Successfully committed 1009
Nov 2 01:19:25 Successfully committed 1010
Nov 2 01:28:16 Successfully committed 1011
```

- To view log entries only for failed batch commit operations, issue the **file show** `/var/log/<filename>` command with the **| match "Error while"** pipe option.

```
user@R0> file show/var/log/commitd_nov | match "Error while"
```

The output shows commit job IDs for failed commit operations.

```
Nov 1 22:47:18 Error while committing 1001
Nov 1 22:51:10 Error while committing 1003
Nov 1 22:52:15 Error while committing 1005
...
```

- To view log entries only for commit server events, issue the **file show** `/var/log/<filename>` command with the **| match "commit server"** pipe option.

```
user@R0> file show/var/log/commitd_nov | match "commit server"
```

The output shows commit server event logs.

```
Nov 1 22:46:39 Commit server status=running
Nov 1 22:46:39 Commit server jobs=1000
Nov 1 22:46:43 Commit server status=not running
Nov 1 22:46:43 Commit server jobs=
Nov 1 22:47:17 Commit server status=running
Nov 1 22:47:18 Commit server jobs=1001
Nov 1 22:47:18 2 errors reported by commit server
Nov 1 22:47:18 Commit server status=not running
Nov 1 22:47:18 Commit server jobs=
Nov 1 22:50:31 Commit server status=running
Nov 1 22:50:31 Commit server jobs=1002
Nov 1 22:50:35 Commit server status=not running
Nov 1 22:50:35 Commit server jobs=
Nov 1 22:51:09 Commit server status=running
Nov 1 22:51:10 Commit server jobs=1003
Nov 1 22:51:10 2 errors reported by commit server
Nov 1 22:51:10 Commit server status=not running
...
```

#### Related Documentation

- [Junos OS Batch Commits Overview on page 516](#)
- [commit-interval \(Batch Commits\) on page 667](#)
- [days-to-keep-error-logs \(Batch Commits\) on page 669](#)
- [maximum-aggregate-pool \(Batch Commits\) on page 679](#)
- [maximum-entries \(Batch Commits\) on page 680](#)
- [maximum-entries on page 680](#)
- [server \(Batch Commits\) on page 688](#)
- [traceoptions \(Batch Commits\) on page 701](#)

# Managing Configurations

- [Understanding How the Junos OS Configuration Is Stored on page 525](#)
- [Comparing Configuration Changes with a Prior Version on page 526](#)
- [Understanding the show | compare | display xml Command Output on page 528](#)
- [Returning to the Most Recently Committed Junos OS Configuration on page 534](#)
- [Returning to a Previously Committed Junos OS Configuration on page 535](#)
- [Saving a Configuration to a File on page 540](#)
- [Additional Details About Specifying Junos OS Statements and Identifiers on page 541](#)
- [Loading a Configuration from a File on page 544](#)
- [Examples: Loading a Configuration from a File on page 547](#)
- [Creating and Returning to a Rescue Configuration on page 549](#)
- [Compressing the Current Configuration File on page 549](#)
- [Example: Protecting the Junos OS Configuration from Modification or Deletion on page 551](#)
- [Synchronizing Routing Engines on page 558](#)
- [Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically on page 560](#)

## Understanding How the Junos OS Configuration Is Stored

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible in the CLI immediately, so if multiple users are editing the configuration at the same time, all users can see all changes.

To have a candidate configuration take effect, you *commit* the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

In addition to saving the current configuration, the CLI saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0, which is the current operational version and the

default configuration that the system returns to if you roll back to a previous configuration. The oldest saved configuration is version 49.

By default, Junos OS saves the current configuration and three previous versions of the committed configuration on the CompactFlash card. The currently operational Junos OS configuration is stored in the file **juniper.conf.gz**, and the last three committed configurations are stored in the files **juniper.conf.1.gz**, **juniper.conf.2.gz**, and **conf.3.gz**. These four files are located in the router or switch's CompactFlash card in the directory **/config**.

The remaining 46 previous versions of committed configurations, the files **juniper.conf.4** through **juniper.conf.49**, are stored in the directory **/var/db/config** on the hard disk.

**Related  
Documentation**

- *Using Junos OS to Specify the Number of Configurations Stored on the CompactFlash Card*
- [Returning to the Most Recently Committed Junos OS Configuration on page 534](#)
- [Returning to a Previously Committed Junos OS Configuration on page 535](#)
- [Loading a Configuration from a File on page 544](#)

---

## Comparing Configuration Changes with a Prior Version

---

In configuration mode only, when you have made changes to the configuration and want to compare the candidate configuration with a prior version, you can use the **compare** command to display the configuration. The **compare** command compares the candidate configuration with either the current committed configuration or a configuration file and displays the differences between the two configurations. To compare configurations, specify the **compare** command after the pipe:

```
[edit]
user@host# show | compare (filename) rollback n
```

**filename** is the full path to a configuration file. The file must be in the proper format: a hierarchy of statements.

**n** is the index into the list of previously committed configurations. The most recently saved configuration is number 0, and the oldest saved configuration is number 49. If you do not specify arguments, the candidate configuration is compared against the active configuration file (**/config/juniper.conf**).

The comparison output uses the following conventions:

- Statements that are only in the candidate configuration are prefixed with a plus sign (+).
- Statements that are only in the comparison file are prefixed with a minus sign (-).
- Statements that are unchanged are prefixed with a single blank space ( ).

The following example shows various changes, then a comparison of the candidate configuration with the active configuration, showing only the changes made at the **[edit protocols bgp]** hierarchy level:

```
[edit]
user@host# edit protocols bgp
[edit protocols bgp]
user@host# show
group my-group {
 type internal;
 hold-time 60;
 advertise-inactive;
 allow 1.1.1.1/32;
}
group fred {
 type external;
 peer-as 33333;
 allow 2.2.2.2/32;
}
group test-peers {
 type external;
 allow 3.3.3.3/32;
}
[edit protocols bgp]
user@host# set group my-group hold-time 90
[edit protocols bgp]
user@host# delete group my-group advertise-inactive
[edit protocols bgp]
user@host# set group fred advertise-inactive
[edit protocols bgp]
user@host# delete group test-peers
[edit protocols bgp]
user@host# show | compare
[edit protocols bgp group my-group]
- hold-time 60;
+ hold-time 90;
- advertise-inactive;
[edit protocols bgp group fred]
+ advertise-inactive;
[edit protocols bgp]
- group test-peers {
 - type external;
 - allow 3.3.3.3/32;
}
[edit protocols bgp]
user@host# show
group my-group {
 type internal;
 hold-time 90;
 allow 1.1.1.1/32;
}
group fred {
 type external;
 advertise-inactive;
 peer-as 33333;
```

```
 allow 2.2.2.2/32;
}
```

**Related  
Documentation**

- [Creating and Returning to a Rescue Configuration on page 538](#)

---

## Understanding the `show | compare | display xml` Command Output

---

The **`compare | display xml`** filter compares the candidate configuration with the current committed configuration and displays the differences between the two configurations in XML. To compare configurations, enter **`compare | display xml`** after the pipe ( `|` ) symbol in either operational or configuration mode.

Example in operational mode:

```
user@host> show configuration | compare | display xml
```

Example in configuration mode:

```
[edit]
user@host# show | compare | display xml
```

You can enter a specific configuration hierarchy immediately preceding the **`compare`** filter, for example, **`show configuration system syslog | compare | display xml`**. In configuration mode, you can navigate to a hierarchy where the command is applied.

The differences from the compare filter function are output in XML. The **`configuration`** tag starts the output. The context for changes is established with hierarchy name tags relative to the root of the compare. For element changes, an **`operation`** attribute are output in the tag where a change occurs. This attribute has the value **`create`**, **`delete`**, or **`merge`**. For metadata changes, the metadata name is specified. For example, if a statement is marked inactive, the **`inactive="inactive"`** attribute and value are output. The `nc` namespace is used when necessary to indicate that an attribute is in the NETCONF namespace rather than the Junos OS namespace.

The following sections explain the XML that is generated for particular types of configuration changes. The corresponding text changes are shown for comparison.

- [Adding a Statement \(create Operation\) on page 529](#)
- [Deleting a Statement \(delete Operation\) on page 529](#)
- [Changing a Statement \(delete and create Operations\) on page 530](#)
- [Changing Metadata \(inactive Attribute and Operation\) on page 531](#)
- [Adding an Annotation \(comment Tag and create Operation\) on page 532](#)
- [Changing an Annotation \(comment Tag, and delete and create Operations\) on page 532](#)
- [Adding a Statement Inside a Container \(create Operation, and insert and key Attributes\) on page 533](#)
- [Changing the Order Inside a Container \(merge Operation, and insert and key Attributes\) on page 534](#)



## Adding a Statement (create Operation)

The following example shows the addition of IPv4 address 2.2.2.2 to unit 1. The tags through **name** provide the context for the addition. The **operation="create"** attribute indicates that a **unit** statement was created and is defined by the configuration within the **unit** tag.

```
[edit interfaces ge-0/0/0]
user@host> show configuration | compare
[edit interfaces ge-0/0/0]
+ unit 1 {
+ family inet {
+ address 2.2.2.2/32;
+ }
+ }

[edit interfaces ge-0/0/0]
user@host# show | compare | display xml
<configuration>
 <interfaces>
 <interface>
 <name>ge-0/0/0</name>
 <unit nc:operation="create">
 <name>1</name>
 <family>
 <inet>
 <address>
 <name>2.2.2.2/32</name>
 </address>
 </inet>
 </family>
 </unit>
 </interface>
 </interfaces>
</configuration>
```

## Deleting a Statement (delete Operation)

The following example shows the deletion of a simple statement in the configuration hierarchy. The tags through **system** provide the context for the deletion. The **operation="delete"** attribute indicates that the **services** statement was deleted. The configuration following the **services** statement was deleted though is not output.

```
[edit system]
user@host> show configuration | compare
[edit system]
- services {
- ftp;
- }

[edit system]
user@host# show | compare | display xml
<configuration>
 <system>
 <services operation="delete"/>
 </system>
</configuration>
```

The following example shows the deletion of unit 1 from the ge-0/0/0 interface. The configuration following the **unit** statement was deleted though is not output.

```
[edit interfaces ge-0/0/0]
user@host> show configuration | compare
[edit interfaces ge-0/0/0]
- unit 1 {
- family inet {
- address 2.2.2.2/32;
- }
- }

[edit interfaces ge-0/0/0]
user@host# show | compare | display xml
<configuration>
 <interfaces>
 <interface>
 <name>ge-0/0/0</name>
 <unit nc:operation="delete">
 <name>1</name>
 </unit>
 </interface>
 </interfaces>
</configuration>
```

The following example shows the deletion of the **apply-groups** configuration. The groups that are deleted are not output.

```
[edit]
user@host# delete apply-groups

[edit]
user@host> show configuration | compare
[edit]
- apply-groups [g1 g2 g3];

[edit]
user@host# show | compare | display xml
<configuration>
 <apply-groups operation="delete"/>
</configuration>
```

## Changing a Statement (delete and create Operations)

The following example shows a change in a statement in the hierarchy. The tags through **system** provide the context for the change. The **operation="delete"** attribute indicates that the **host-name** statement was deleted. The configuration following the **host-name** statement was deleted though is not output. The **operation="create"** attribute indicates that a **host-name** statement was created and is defined by the configuration within the **host-name** tag.

```
[edit system]
user@host> show configuration | compare
[edit system]
- host-name router1;
+ host-name router2;

[edit system]
user@host# show | compare | display xml
```

```

<configuration>
 <system>
 <host-name nc:operation="delete"/>
 <host-name nc:operation="create">router2</host-name>
 </system>
</configuration>

```

## Changing Metadata (inactive Attribute and Operation)

The following example shows the inactivation of a statement in the hierarchy. The tags through **system** provide the context for the change. The **inactive="inactive"** attribute indicates that the **syslog** statement was inactivated.

```

[edit system]
user@host> show configuration | compare
[edit system]
! inactive: syslog { ... }

[edit system]
user@host# show | compare | display xml
<configuration>
 <system>
 <syslog inactive="inactive"/>
 </system>
</configuration>

```

The following example shows the addition of an inactive **syslog** statement. The **operation="create"** attribute indicates that the **syslog** statement was created and is defined by the configuration within the **syslog** tag. The **inactive="inactive"** attribute indicates that the **syslog** statement was inactivated.

```

[edit system]
user@host> show configuration | compare
[edit system]
+ inactive: syslog {
+ file foo {
+ any any;
+ }
+ }

[edit system]
user@host# show | compare | display xml
<configuration>
 <system>
 <syslog nc:operation="create"
 inactive="inactive">
 <file>
 <name>foo</name>
 <contents>
 <name>any</name>
 <any/>
 </contents>
 </file>
 </syslog>
 </system>
</configuration>

```

## Adding an Annotation (comment Tag and create Operation)

The following example shows the addition of a comment to a statement. The tags through **syslog** provide the context for the annotation. The **operation="create"** attribute for the **junos:comment** tag indicates that a comment was added to the **[edit system syslog]** hierarchy.

```
[edit system]
user@host> show configuration | compare
[edit system]
+ /* my-comments-simple */
 syslog { ... }

[edit system]
user@host# show | compare | display xml
<configuration>
 <system>
 <junos:comment nc:operation="create">/* my-comments-simple
 */</junos:comment>
 <syslog/>
 </system>
</configuration>
```

The following example shows the addition of a comment to a statement. The tags through **syslog** provide the context for the annotation. The **operation="create"** attribute for the **junos:comment** tag indicates that a comment was added to the **[edit system syslog]** hierarchy for the statement output within the **syslog** tag.

```
[edit system syslog]
user@host> show configuration | compare
+ /* my-comments-ele */
 file f1 { ... }

[edit system syslog]
user@host# show | compare | display xml
<configuration>
 <system>
 <syslog>
 <junos:comment nc:operation="create">/* my-comments-elem
 */</junos:comment>
 <file>
 <name>f1</name>
 </file>
 </syslog>
 </system>
</configuration>
```

## Changing an Annotation (comment Tag, and delete and create Operations)

The following example shows the change of a comment for a statement. The tags through **system** provide the context for the annotation. The **operation="delete"** attribute for the **junos:comment** tag indicates that a comment was deleted from the **[edit system]** hierarchy at the **syslog** statement. The **operation="create"** attribute for the **junos:comment** tag

indicates that a comment was added to the **[edit system]** hierarchy for the **syslog** statement.

```
[edit system]
user@host> show configuration | compare
- /* my-comments-1 */
+ /* my-comments-2 */
 syslog { ... }

[edit system]
user@host# show | compare | display xml
<configuration>
 <system>
 <junos:comment nc:operation="delete"/>
 <junos:comment nc:operation="create">/* my-comments-2
*/</junos:comment>
 <syslog/>
 </system>
</configuration>
```

### Adding a Statement Inside a Container (create Operation, and insert and key Attributes)

The following example shows the addition of a **file** statement at the **[edit system syslog]** hierarchy. The tags through **syslog** provide the context for the addition. The **operation="create"** attribute for the **file** tag indicates that a **file** statement was added. The **yang:insert="after"** attribute indicates that the file was added after the position indicated by the **yang:key="[name='file-1']"** attribute. The **file-1** value represents the position within the existing **file** statements, where one is the first file. In this example, the new **file** statement was added after the first file.

```
[edit system syslog]
user@host> show configuration | compare
[edit system syslog]
 file file-1 { ... }
+ file file-2 {
+ any any;
+ }

[edit system syslog]
user@host# show | compare | display xml
<configuration>
 <system>
 <syslog>
 <file nc:operation="create"
 yang:insert="after"
 yang:key="[name='file-1']">
 <name>file-2</name>
 <contents>
 <name>any</name>
 <any/>
 </contents>
 </file>
 </syslog>
 </system>
</configuration>
```

## Changing the Order Inside a Container (merge Operation, and insert and key Attributes)

The following example shows the change in order of **file** statements at the **[edit system syslog]** hierarchy. The tags through **syslog** provide the context for the change. The **operation="merge"** attribute for the **file** tag indicates that an existing **file** statement was moved. The **yang:insert="after"** attribute indicates that the file was moved after the file in the position indicated by the **yang:key="[name='file-1']"** attribute. The **file-1** value represents a position within the existing **file** statements, where one is the first file. The value at the **name** tag, **file-3**, represents a position within the existing file statements. In this example, the **file** statement in the third position was moved after the first file.

```
[edit system syslog]
user@host> show configuration | compare
[edit system syslog]
 file f1 { ... }
! file f3 { ... }

[edit system syslog]
user@host# show | compare | display xml
<configuration>
 <system>
 <syslog>
 <file nc:operation="merge"
 yang:insert="after"
 yang:key="[name='file-1']">
 <name>file-3</name>
 </file>
 </syslog>
 </system>
 </configuration>
```

### Related Documentation

- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos OS Command Output on page 588](#)
- [Pipe \( | \) Filter Functions in the Junos OS Command-Line Interface on page 590](#)
- [Using the Pipe \( | \) Symbol to Filter Junos OS Command Output on page 587](#)

## Returning to the Most Recently Committed Junos OS Configuration

---

To return to the most recently committed configuration and load it into configuration mode without activating it, use the **rollback** configuration mode command:

```
[edit]
user@host# rollback

load complete
```

To activate the configuration to which you rolled back, use the **commit** command:

```
[edit]
user@host# rollback
load complete
[edit]
user@host# commit
```

- Related Documentation**
- [Rolling Back Junos OS Configuration Changes on page 444](#)
  - [Returning to a Previously Committed Junos OS Configuration on page 535](#)
  - [Understanding How the Junos OS Configuration Is Stored on page 525](#)

## Returning to a Previously Committed Junos OS Configuration

This topic explains how you can return to a configuration prior to the most recently committed one, and contains the following sections:

- [Returning to a Configuration Prior to the One Most Recently Committed on page 535](#)
- [Displaying Previous Configurations on page 535](#)
- [Comparing Configuration Changes with a Prior Version on page 536](#)
- [Creating and Returning to a Rescue Configuration on page 538](#)
- [Saving a Configuration to a File on page 539](#)

### Returning to a Configuration Prior to the One Most Recently Committed

To return to a configuration prior to the most recently committed one, include the configuration number, 0 through 49, in the **rollback** command. The most recently saved configuration is number 0 (which is the default configuration to which the system returns), and the oldest saved configuration is number 49.

```
[edit]
user@host# rollback number
load complete
```

### Displaying Previous Configurations

To display previous configurations, including the rollback number, date, time, the name of the user who committed changes, and the method of commit, use the **rollback ?** command.

```
[edit]
user@host# rollback ?
Possible completions:
<[Enter]> Execute this command
<number> Numeric argument
0 2005-02-27 12:52:10 PST by abc via cli
1 2005-02-26 14:47:42 PST by def via cli
2 2005-02-14 21:55:45 PST by ghi via cli
3 2005-02-10 16:11:30 PST by jkl via cli
4 2005-02-10 16:02:35 PST by mno via cli
5 2005-03-16 15:10:41 PST by pqr via cli
6 2005-03-16 14:54:21 PST by stu via cli
7 2005-03-16 14:51:38 PST by vwx via cli
8 2005-03-16 14:43:29 PST by yzz via cli
9 2005-03-16 14:15:37 PST by abc via cli
10 2005-03-16 14:13:57 PST by def via cli
11 2005-03-16 12:57:19 PST by root via other
12 2005-03-16 10:45:23 PST by root via other
```

```

13 2005-03-16 10:08:13 PST by root via other
14 2005-03-16 01:20:56 PST by root via other
15 2005-03-16 00:40:37 PST by ghi via cli
16 2005-03-16 00:39:29 PST by jkl via cli
17 2005-03-16 00:32:36 PST by mno via cli
18 2005-03-16 00:31:17 PST by pqr via cli
19 2005-03-15 19:59:00 PST by stu via cli
20 2005-03-15 19:53:39 PST by vwx via cli
21 2005-03-15 18:07:19 PST by yzz via cli
22 2005-03-15 17:59:03 PST by abc via cli
23 2005-03-15 15:05:14 PST by def via cli
24 2005-03-15 15:04:51 PST by ghi via cli
25 2005-03-15 15:03:42 PST by jkl via cli
26 2005-03-15 15:01:52 PST by mno via cli
27 2005-03-15 14:58:34 PST by pqr via cli
28 2005-03-15 13:09:37 PST by root via other
29 2005-03-12 11:01:20 PST by stu via cli
30 2005-03-12 10:57:35 PST by vwx via cli
31 2005-03-11 10:25:07 PST by yzz via cli
32 2005-03-10 23:40:58 PST by abc via cli
33 2005-03-10 23:40:38 PST by def via cli
34 2005-03-10 23:14:27 PST by ghi via cli
35 2005-03-10 23:10:16 PST by jkl via cli
36 2005-03-10 23:01:51 PST by mno via cli
37 2005-03-10 22:49:57 PST by pqr via cli
38 2005-03-10 22:24:07 PST by stu via cli
39 2005-03-10 22:20:14 PST by vwx via cli
40 2005-03-10 22:16:56 PST by yzz via cli
41 2005-03-10 22:16:41 PST by abc via cli
42 2005-03-10 20:44:00 PST by def via cli
43 2005-03-10 20:43:29 PST by ghi via cli
44 2005-03-10 20:39:14 PST by jkl via cli
45 2005-03-10 20:31:30 PST by root via other
46 2005-03-10 18:57:01 PST by mno via cli
47 2005-03-10 18:56:18 PST by pqr via cli
48 2005-03-10 18:47:49 PST by stu via cli
49 2005-03-10 18:47:34 PST by vw via cli
| Pipe through a command
[edit]

```

## Comparing Configuration Changes with a Prior Version

In configuration mode only, when you have made changes to the configuration and want to compare the candidate configuration with a prior version, you can use the **compare** command to display the configuration. The **compare** command compares the candidate configuration with either the current committed configuration or a configuration file and displays the differences between the two configurations. To compare configurations, specify the **compare** command after the pipe:

```

[edit]
user@host# show | compare (filename| rollback n)

```

**filename** is the full path to a configuration file. The file must be in the proper format: a hierarchy of statements.



*n* is the index into the list of previously committed configurations. The most recently saved configuration is number 0, and the oldest saved configuration is number 49. If you do not specify arguments, the candidate configuration is compared against the active configuration file (`/config/juniper.conf`).

The comparison output uses the following conventions:

- Statements that are only in the candidate configuration are prefixed with a plus sign (+).
- Statements that are only in the comparison file are prefixed with a minus sign (-).
- Statements that are unchanged are prefixed with a single blank space ( ).

The following example shows various changes, then a comparison of the candidate configuration with the active configuration, showing only the changes made at the **[edit protocols bgp]** hierarchy level:

```
[edit]
user@host# edit protocols bgp
[edit protocols bgp]
user@host# show
group my-group {
 type internal;
 hold-time 60;
 advertise-inactive;
 allow 1.1.1.1/32;
}
group fred {
 type external;
 peer-as 33333;
 allow 2.2.2.2/32;
}
group test-peers {
 type external;
 allow 3.3.3.3/32;
}
[edit protocols bgp]
user@host# set group my-group hold-time 90
[edit protocols bgp]
user@host# delete group my-group advertise-inactive
[edit protocols bgp]
user@host# set group fred advertise-inactive
[edit protocols bgp]
user@host# delete group test-peers
[edit protocols bgp]
user@host# show | compare
[edit protocols bgp group my-group]
-hold-time 60;
+hold-time 90;
-advertise-inactive;
[edit protocols bgp group fred]
+advertise-inactive;
[edit protocols bgp]
-group test-peers {
```

```
-type external;
-allow 3.3.3.3/32;
}
[edit protocols bgp]
user@host# show
group my-group {
 type internal;
 hold-time 90;
 allow 1.1.1.1/32;
}
group fred {
 type external;
 advertise-inactive;
 peer-as 3333;
 allow 2.2.2.2/32;
}
```

## Creating and Returning to a Rescue Configuration

A rescue configuration allows you to define a known working configuration or a configuration with a known state that you can roll back to at any time. This alleviates the necessity of having to remember the rollback number with the **rollback** command. You use the rescue configuration when you need to roll back to a known configuration or as a last resort if your router or switch configuration and the backup configuration files become damaged beyond repair.

To save the most recently committed configuration as the rescue configuration so that you can return to it at any time, issue the **request system configuration rescue save** command:

```
user@host> request system configuration rescue save
```

To return to the rescue configuration, use the **rollback rescue** configuration mode command:

```
[edit]
user@host# rollback rescue
load complete
```



**NOTE:** If the rescue configuration does not exist, or if the rescue configuration is not a complete, viable configuration, then the rollback command fails, an error message appears, and the current configuration remains active.

To activate the rescue configuration that you have loaded, use the **commit** command:

```
[edit]
user@host# rollback rescue
load complete
[edit]
user@host# commit
```

To delete an existing rescue configuration, issue the **request system configuration rescue delete** command:

```
user@host> request system configuration rescue delete
user@host>
```

For more information about the **request system configuration rescue delete** and **request system configuration rescue save** commands, see the [CLI Explorer](#).

## Saving a Configuration to a File

Save Junos OS configuration to a file so that you can edit it with a text editor of your choice. You can save your current configuration to an ASCII file, which saves the configuration in its current form, including any uncommitted changes. If more than one user is modifying the configuration, all changes made by all users are saved.

To save software configuration changes to an ASCII file, use the **save** configuration mode command:

```
[edit]
user@host# save filename
[edit]
user@host#
```

The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy.

By default, the configuration is saved to a file in your home directory, which is on the flash drive.

When you issue this command from anywhere in the hierarchy (except the top level), a **replace** tag is automatically included at the beginning of the file. You can use the **replace** tag to control how a configuration is loaded from a file.

```
user@host> file show /var/home/user/myconf
replace:
protocols {
 bgp {
 disable;
 group int {
 type internal;
 }
 }
 isis {
 disable;
 interface all {
 level 1 disable;
 }
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 traffic-engineering;
 reference-bandwidth 4g;
 ...
 }
}
```

```
}
```

**Related Documentation**

- [Returning to the Most Recently Committed Junos OS Configuration on page 534](#)
- [Loading a Configuration from a File on page 544](#)
- [Specifying Filenames and URLs on page 576](#)

---

## Saving a Configuration to a File

Save Junos OS configuration to a file so that you can edit it with a text editor of your choice. You can save your current configuration to an ASCII file, which saves the configuration in its current form, including any uncommitted changes. If more than one user is modifying the configuration, all changes made by all users are saved.

To save software configuration changes to an ASCII file, use the **save** configuration mode command:

```
[edit]
user@host# save filename
[edit]
user@host#
```

The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy.

By default, the configuration is saved to a file in your home directory, which is on the flash drive.

When you issue this command from anywhere in the hierarchy (except the top level), a **replace** tag is automatically included at the beginning of the file. You can use the **replace** tag to control how a configuration is loaded from a file.

```
user@host> file show /var/home/user/myconf
replace:
protocols {
 bgp {
 disable;
 group int {
 type internal;
 }
 }
 isis {
 disable;
 interface all {
 level 1 disable;
 }
 interface fxp0.0 {
 disable;
 }
 }
 ospf {
 traffic-engineering;
```

```

 reference-bandwidth 4g;
 ...
}
}

```

## Additional Details About Specifying Junos OS Statements and Identifiers

This topic provides more detailed information about CLI container and leaf statements so that you can better understand how you must specify them when creating ASCII configuration files. It also describes how the CLI performs type checking to verify that the data you entered is in the correct format.

- [Specifying Statements on page 541](#)
- [Performing CLI Type Checking on page 543](#)

### Specifying Statements

Statements are shown one of two ways, either with braces or without:

- Statement name and identifier, with one or more lower level statements enclosed in braces:

```

statement-name1 identifier-name {
 statement-name2;
 additional-statements;
}

```

- Statement name, identifier, and a single identifier:

```

statement-name identifier-name1 identifier-name2;

```

The **statement-name** is the name of the statement.

The **identifier-name** is a name or other string that uniquely identifies an instance of a statement. An identifier is used when a statement can be specified more than once in a configuration.

When specifying a statement, you must specify either a statement name or an identifier name, or both, depending on the statement hierarchy.

You specify identifiers in one of the following ways:

- **identifier-name**—The **identifier-name** is a keyword used to uniquely identify a statement when a statement can be specified more than once in a statement.
- **identifier-name value**—The **identifier-name** is a keyword, and the **value** is a required option variable.
- **identifier-name [value1 value2 value3 ...]**—The **identifier-name** is a keyword that accepts multiple values. The brackets are required when you specify a set of values; however, they are optional when you specify only one value.

The following examples illustrate how statements and identifiers are specified in the configuration:

```
protocol { # Top-level statement (statement-name).
 ospf { # Statement under "protocol" (statement-name).
 area 0.0.0.0 { # OSPF area "0.0.0.0" (statement-name identifier-name),
 interface so-0/0/0 { # which contains an interface named "so-0/0/0."
 hello-interval 25; # Identifier and value (identifier-name value).
 priority 2; # Identifier and value (identifier-name value).
 disable; # Flag identifier (identifier-name).
 }
 interface so-0/0/1; # Another instance of "interface," named so-0/0/1,
 } # this instance contains no data, so no braces
 } # are displayed.
}

policy-options { # Top-level statement (statement-name).
 term term1 { # Statement under "policy-options"
 # (statement-name value).
 from { # Statement under "term" (statement-name).
 route-filter 10.0.0.0/8 orlonger reject; # One identifier ("route-filter")
 with
 route-filter 127.0.0.0/8 orlonger reject; # multiple values.
 route-filter 128.0.0.0/16 orlonger reject;
 route-filter 149.20.64.0/24 orlonger reject;
 route-filter 172.16.0.0/12 orlonger reject;
 route-filter 191.255.0.0/16 orlonger reject;
 }
 then { # Statement under "term" (statement-name).
 next term; # Identifier (identifier-name).
 }
 }
}
```

When you create an ASCII configuration file, you can specify statements and identifiers in one of the following ways. However, each statement has a preferred style, and the CLI uses that style when displaying the configuration in response to a configuration mode **show** command.

- Statement followed by identifiers:

```
statement-name identifier-name [...] identifier-name value [...];
```

- Statement followed by identifiers enclosed in braces:

```
statement-name {
 identifier-name;
 [...]
 identifier-name value;
 [...]
}
```

- For some repeating identifiers, you can use one set of braces for all the statements:

```
statement-name {
 identifier-name value1;
 identifier-name value2;
}
```

## Performing CLI Type Checking

When you specify identifiers and values, the CLI performs type checking to verify that the data you entered is in the correct format. For example, for a statement in which you must specify an IP address, the CLI requires you to enter an address in a valid format. If you have not, an error message indicates what you need to type. [Table 60](#) lists the data types the CLI checks.

**Table 60: CLI Configuration Input Types**

| Data Type                                                                                                   | Format                                                                                         | Examples                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physical interface name (used in the <code>[edit interfaces]</code> hierarchy)                              | <i>type-fpc/pic/port</i>                                                                       | Correct: so-0/0/1<br>Incorrect: so-0                                                                                                                                                                              |
| Full interface name                                                                                         | <i>type-fpc/pic/port&lt;:channel&gt;.logical</i>                                               | Correct: so-0/0/1.0<br>Incorrect: so-0/0/1                                                                                                                                                                        |
| Full or abbreviated interface name (used in places other than the <code>[edit interfaces]</code> hierarchy) | <i>type-&lt;fpc&lt;/pic/port&gt;&gt;&lt;&lt;:channel&gt;.logical&gt;</i>                       | Correct: so, so-1, so-1/2/3:4.5                                                                                                                                                                                   |
| IP address                                                                                                  | <i>0xhex-bytesoctet&lt;.octet&lt;.octet.&lt;octet&gt;&gt;&gt;</i>                              | Correct: 1.2.3.4, 0x01020304, 128.8.1, 128.8<br><br>Sample translations:<br><br>1.2.3 becomes 1.2.3.0<br>0x01020304 becomes 1.2.3.4<br>0x010203 becomes 0.1.2.3                                                   |
| IP address (destination prefix) and prefix length                                                           | <i>0xhex-bytes&lt;/length&gt;octet&lt;octet&lt;.octet.&lt;octet&gt;&gt;&gt;&lt;/length&gt;</i> | Correct: 10/8, 128.8/16, 1.2.3.4/32, 1.2.3.4<br><br>Sample translations:<br><br>1.2.3 becomes 1.2.3.0/32<br>0x01020304 becomes 1.2.3.4/32<br>0x010203 becomes 0.1.2.3/32<br>default becomes 0.0.0.0/0             |
| International Organization for Standardization (ISO) address                                                | <i>hex-nibble&lt;hex-nibble ...&gt;</i>                                                        | Correct: 47.1234.2345.3456.00, 47.1234.2345.34.56.00, 47.12.34.23.45.34.56.00<br><br>Sample translations:<br><br>47.123456 becomes 47.1234.56<br>47.12.34.56 becomes 47.1234.56<br>47.12.34.56 becomes 47.1234.56 |

Table 60: CLI Configuration Input Types (*continued*)

| Data Type                 | Format                                                                             | Examples                                                                                                                                                                                           |
|---------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSPF area identifier (ID) | <i>0xhex-bytesoctet&lt;.octet&lt;.octet.&lt; octet &gt;&gt;&gt; decimal-number</i> | <p>Correct: 54, 0.0.0.54, 0x01020304, 1.2.3.4</p> <p>Sample translations:</p> <p>54 becomes 0.0.0.54</p> <p>257 becomes 0.0.1.1</p> <p>128.8 becomes 128.8.0.0</p> <p>0x010203 becomes 0.1.2.3</p> |

**Related Documentation** • [Entering and Exiting the Junos OS CLI Configuration Mode on page 462](#)

## Loading a Configuration from a File

You can create a file, copy the file to the local router, and then load the file into the CLI. After you have loaded the file, you can commit it to activate the configuration on the router, or you can edit the configuration interactively using the CLI and commit it at a later time.

You can also create a configuration while typing at the terminal and then load it. Loading a configuration from the terminal is generally useful when you are cutting existing portions of the configuration and pasting them elsewhere in the configuration.

To load an existing configuration file that is located on the router, use the **load** configuration mode command:

```
[edit]
user@host# load (factory-default | merge | override | patch | replace | set | update)
filename <relative>
```

For information about specifying the filename, see [“Specifying Filenames and URLs” on page 576](#).

To load a configuration from the terminal, use the following version of the **load** configuration mode command. Press Ctrl-d to end the input.

```
[edit]
user@host# load (factory-default | merge | override | patch | replace | set | update)
terminal <relative>
```

To replace an entire configuration, specify the **override** option at any level of the hierarchy. A **load override** operation completely replaces the current candidate configuration with the file you are loading. Thus, if you saved a complete configuration, use this option.

An **override** operation discards the current candidate configuration and loads the configuration in **filename** or the configuration that you type at the terminal. When you use the **override** option and commit the configuration, all system processes reparse the configuration. For an example, see [Figure 15](#).



To replace portions of a configuration, specify the **replace** option. The **load replace** operation looks for **replace:** tags that you added to the loaded file, and replaces the parts of the candidate configuration with whatever is specified after the tag. This is useful when you want more control over exactly what is being changed. For this operation to work, you must include **replace:** tags in the file or configuration you type at the terminal. The software searches for the **replace:** tags, deletes the existing statements of the same name, if any, and replaces them with the incoming configuration. If there is no existing statement of the same name, the **replace** operation adds to the configuration the statements marked with the **replace:** tag. For an example, see [Figure 16](#).

If, in an **override** or **merge** operation, you specify a file or type text that contains **replace:** tags, the **replace:** tags are ignored and the **override** or **merge** operation is performed.

If you are performing a **replace** operation and the file you specify or text you type does not contain any **replace:** tags, the **replace** operation is effectively equivalent to a **merge** operation. This might be useful if you are running automated scripts and cannot know in advance whether the scripts need to perform a **replace** or a **merge** operation. The scripts can use the **replace** operation to cover either case.

The **load merge** operation adds the saved file to the existing candidate configuration. This is useful if you are adding new configuration sections. For example, suppose that you are adding a BGP configuration to the **[edit protocols]** hierarchy level, where there was no BGP configuration before, you can use the **load merge** operation to combine the saved file configuration to the existing candidate configuration. If the existing configuration and the incoming configuration contain conflicting statements, the statements in the incoming configuration override those in the existing configuration.

To replace only the configuration that has changed, specify the **update** option at any level of the hierarchy. The **load update** operation compares the candidate configuration and the file you are loading, and only changes the parts of the candidate configuration that are different from the new configuration. You would use this, for example, if there is an existing BGP configuration and the file you are loading changes it in some way.

To change part of the configuration with a patch file, specify the **patch** option. The **load patch** operation loads a file or terminal input that contains configuration changes. First, on a device that already has the configuration changes, you type the **show | compare** command to output the differences between two configurations. Then you can load the differences on another router. The advantage of the **load patch** command is that it saves you from having to copy snippets from different hierarchy levels into a text file prior to loading them into the target device. This might be a useful time saver if you are configuring several devices with the same options. For example, suppose that you configure a routing policy on router1 and you want to replicate the policy configuration on router2, router3, and router4. You can use the **load patch** operation.

First, run the **show | compare** command.

```
user@router1# show | compare rollback 3
[edit protocols ospf]
+ export default-static;
- export static-default
[edit policy-options]
+ policy-statement default-static {
```

```
+ from protocol static;
+ then accept;
+ }
```

Copy the output of the **show | compare** command to the clipboard, making sure to include the hierarchy levels. On router2, router3, and router4, type **load patch terminal** and paste the output. Press Enter and then press Ctrl-d to end the operation. If the patch input specifies different values for an existing statement, the patch input overrides the existing statement.

To use the **merge**, **replace**, **set**, or **update** option without specifying the full hierarchy level, specify the **relative** option. For example:

```
[edit system]
user@host# show static-host-mapping
bob sysid 987.654.321ab
[edit system]
user@host# load replace terminal relative
[Type ^D at a new line to end input]
replace: static-host-mapping {
 bob sysid 0123.456.789bc;
}
load complete
[edit system]
user@host# show static-host-mapping
bob sysid 0123.456.789bc;
```

To load a configuration that contains the **set** configuration mode command, specify the **set** option. This option executes the configuration instructions line by line as they are stored in a file or from a terminal. The instructions can contain any configuration mode command, such as **set**, **edit**, **exit**, and **top**. For an example, see [Figure 19](#).

To copy a configuration file from another network system to the local router, you can use the SSH and Telnet utilities, as described in the [CLI Explorer](#).



**NOTE:** If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

```
load merge
load replace
load override
load update
```

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

#### Related Documentation

- [Examples: Loading a Configuration from a File on page 547](#)

Examples: Loading a Configuration from a File

Figure 15: Overriding the Current Configuration



Figure 16: Using the replace Option

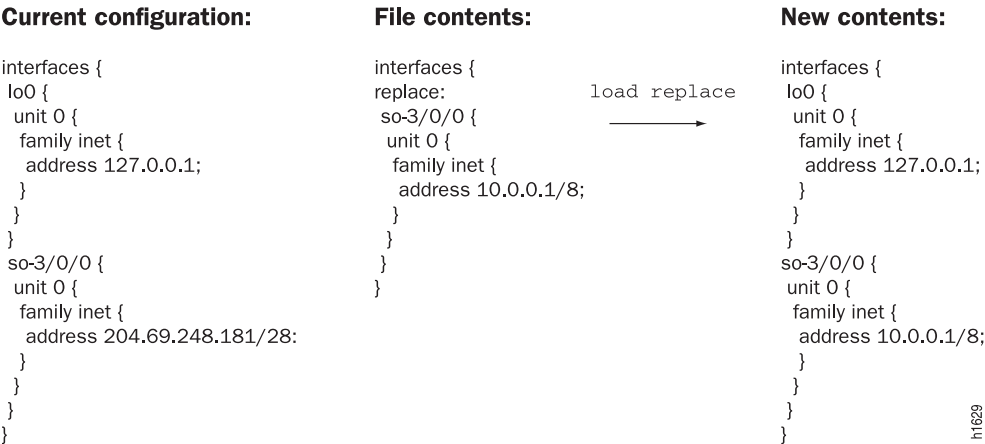
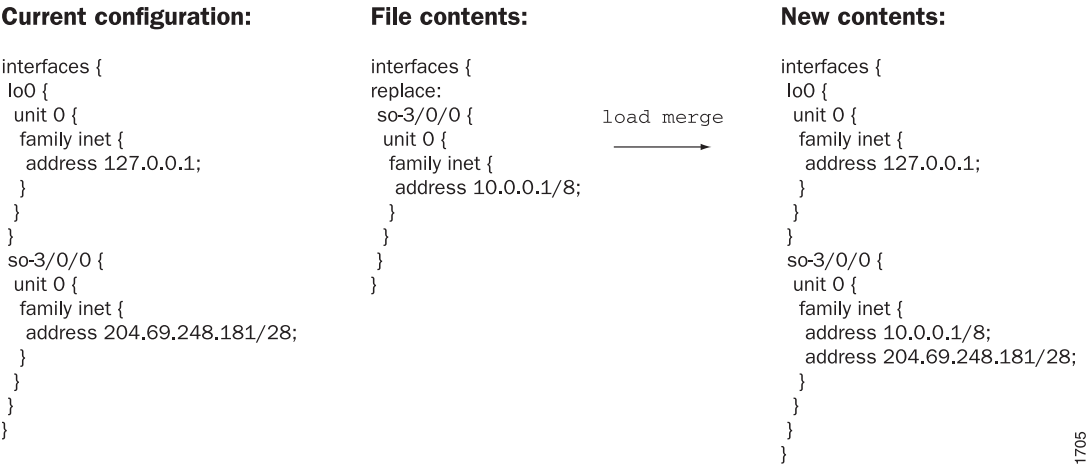


Figure 17: Using the merge Option



**Figure 18: Using a Patch File****Current configuration:**

```

interfaces {
 fxp0 {
 unit 0 {
 family inet {
 address 192.168.6.193/24;
 }
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 127.0.0.1/32;
 }
 }
 }
}

```

**File contents:**

```

(edit interfaces)
+ so-0/0/0 {
+ unit 0 {
+ family inet {
+ address 10.0.0.1/8;
+ }
+ }
+ }

```

load patch

**New contents:**

```

interfaces {
 so-0/0/0 {
 unit 0 {
 family inet {
 address 10.0.0.1/8;
 }
 }
 }
 fxp0 {
 unit 0 {
 family inet {
 address 192.168.6.193/24;
 }
 }
 }
 lo0 {
 unit 0 {
 family inet {
 address 127.0.0.1/32;
 }
 }
 }
}

```

h1969

**Figure 19: Using the set Option****File contents:**

```

edit access
set profile p1 client cl ike
edit profile p1 client cl ike
set pre-shared-key ascii-text "abcd"
set allowed-proxy-pair local 1.1.1.1 remote 2.2.2.2
exit
deactivate profile p1
top
edit system
set radius-server 1.1.1.1

```

load set

**New contents:**

```

system {
 radius-server {
 1.1.1.1;
 }
}
access {
 inactive: profile p1 {
 client cl {
 ike {
 allowed-proxy-pair local 1.1.1.1/32 remote 2.2.2.2/32;
 pre-shared-key ascii-text "9Ydg4ZDjqf5FVw"; ## SECRET-DATA
 }
 }
 }
}
}

```

g017215

**Related Documentation**

- [Loading a Configuration from a File on page 544](#)

## Creating and Returning to a Rescue Configuration

A rescue configuration allows you to define a known working configuration or a configuration with a known state that you can roll back to at any time. This alleviates the necessity of having to remember the rollback number with the **rollback** command. You use the rescue configuration when you need to roll back to a known configuration or as a last resort if your router or switch configuration and the backup configuration files become damaged beyond repair.

To save the most recently committed configuration as the rescue configuration so that you can return to it at any time, issue the **request system configuration rescue save** command:

```
user@host> request system configuration rescue save
```

To return to the rescue configuration, use the **rollback rescue** configuration mode command:

```
[edit]
user@host# rollback rescue
load complete
```



**NOTE:** If the rescue configuration does not exist, or if the rescue configuration is not a complete, viable configuration, then the **rollback** command fails, an error message appears, and the current configuration remains active.

To activate the rescue configuration that you have loaded, use the **commit** command:

```
[edit]
user@host# rollback rescue
load complete
[edit]
user@host# commit
```

To delete an existing rescue configuration, issue the **request system configuration rescue delete** command:

```
user@host> request system configuration rescue delete
user@host>
```

For more information about the **request system configuration rescue delete** and **request system configuration rescue save** commands, see the [CLI Explorer](#).

### Related Documentation

- [Comparing Configuration Changes with a Prior Version on page 526](#)
- [Saving a Configuration to a File on page 539](#)

## Compressing the Current Configuration File

By default, the current operational configuration file is compressed and is stored in the file **juniper.conf.gz** the **/config** file system, along with the last three committed versions

of the configuration. If you have large networks, the current configuration file might exceed the available space in the **/config** file system. Compressing the current configuration file enables the file to fit in the file system, typically reducing the size of the file by 90 percent. You might want to compress your current operation configuration files when they reach 3 megabytes (MB) in size.

When you compress the current configuration file, the names of the configuration files change. To determine the size of the files in the **/config** file system, issue the **file list /config detail** command.



**NOTE:** We recommend that you compress the configuration files (this is the default) to minimize the amount of disk space that they require.

- If you want to compress the current configuration file, include the **compress-configuration-files** statement at the **[edit system]** hierarchy level:  

```
[edit system]
compress-configuration-files;
```
- Commit the current configuration file to include the **compression-configuration-files** statement. Commit the configuration again to compress the current configuration file:

```
[edit system]
user@host# set compress-configuration-files
user@host# commit
commit complete
user@host# commit
commit complete
```

- If you do not want to compress the current operational configuration file, include the **no-compress-configuration-files** statement at the **[edit system]** hierarchy level:  

```
[edit system]
no-compression-configuration-files;
```
- Commit the current configuration file to include the **no-compress-configuration-files** statement. Commit the configuration again to uncompress the current configuration file:

```
[edit system]
user@host# commit
commit complete
user@host# commit
commit complete
```

**Related  
Documentation**

- [Junos OS Commit Model for Router or Switch Configuration on page 507](#)
- [compress-configuration-files](#)

## Example: Protecting the Junos OS Configuration from Modification or Deletion

---

This example shows how to use the **protect** and **unprotect** commands in the configuration mode to protect and unprotect the CLI configuration.

- [Requirements on page 551](#)
- [Overview on page 551](#)
- [Protecting a Parent-Level Hierarchy on page 552](#)
- [Protecting a Child Hierarchy on page 552](#)
- [Protecting a Configuration Statement Within a Hierarchy on page 552](#)
- [Protecting a List of Identifiers for a Configuration Statement on page 553](#)
- [Protecting an Individual Member from a Homogenous List on page 553](#)
- [Unprotecting a Configuration on page 554](#)
- [Verification on page 554](#)

### Requirements

This example uses the following hardware and software components:

- A M Series, MX Series, PTX Series, or T Series device
- Junos OS 11.2 or later running on all devices

### Overview

The Junos OS enables you to protect the device configuration from being modified or deleted by other users. This can be accomplished by using the **protect** command in the configuration mode of the CLI. Likewise, you can also unprotect a protected configuration by using the **unprotect** command.

These commands can be used at any level of the configuration hierarchy—a top-level parent hierarchy or a configuration statement or an identifier within the lowest level of the hierarchy.

If a configuration hierarchy is protected, users cannot perform the following activities:

- Deleting or modifying a hierarchy or a statement or identifier within the protected hierarchy
- Inserting a new configuration statement or an identifier within the protected hierarchy
- Renaming a statement or identifier within the protected hierarchy
- Copying a configuration into a protected hierarchy
- Activating or deactivating statements within a protected hierarchy
- Annotating a protected hierarchy

## Protecting a Parent-Level Hierarchy

- Step-by-Step Procedure** To protect a configuration at the top level of the hierarchy:
- Identify the hierarchy that you want to protect and issue the **protect** command for the hierarchy at the **[edit]** hierarchy level.
- For example, if you want to protect the entire **[edit access]** hierarchy level, issue the following command:
- ```
[edit]
user@host# protect access
```
- Results** Protects all elements under the parent hierarchy.



NOTE:

- If you issue the **protect** command for a hierarchy that is not used in the configuration, the Junos OS CLI displays the following error message:
- ```
[edit]
user@host# protect access
warning: statement not found
```
- 

## Protecting a Child Hierarchy

- Step-by-Step Procedure** To protect a child hierarchy contained within a parent hierarchy:
- Navigate to the parent container hierarchy. Use the **protect** command for the hierarchy at the parent level.
- For example, if you want to protect the **[edit system syslog console]** hierarchy level, use the following command at the **[edit system syslog]** hierarchy level.
- ```
[edit system syslog]
user@host# protect console
```
- Results** Protects all elements under the child hierarchy.

Protecting a Configuration Statement Within a Hierarchy

- Step-by-Step Procedure** To protect a configuration statement within a hierarchy level:
- Navigate to the hierarchy level containing the statement that you want to protect and issue the **protect** command for the hierarchy.
- For example, if you want to protect the **host-name** statement under the **[edit system]** hierarchy level, issue the following command:
- ```
[edit system]
user@host# protect host-name
```



## Protecting a List of Identifiers for a Configuration Statement

**Step-by-Step Procedure** Some configuration statements can take multiple values. For example, the **address** statement at the **[edit system login deny-sources]** hierarchy level can take a list of hostnames, IPv4 addresses, or IPv6 addresses. Suppose you have the following configuration:

```
[edit system login]
deny-sources {
 address [172.17.28.19 172.17.28.20 172.17.28.21 172.17.28.22];
}
```

- To protect all the addresses for the **address** statement, issue the following command at the **[edit]** level:

```
[edit]
user@host# protect system login deny-sources address
```

**Results** All the addresses ([172.17.28.19 172.17.28.20 172.17.28.21 172.17.28.22]) for the **address** statement are protected.

## Protecting an Individual Member from a Homogenous List

**Step-by-Step Procedure** Suppose you have the following configuration:

```
[edit groups]
test1 {
 system {
 name-server {
 10.1.2.1;
 10.1.2.2;
 10.1.2.3;
 10.1.2.4;
 }
 }
}
```

- To protect one or more individual addresses for the **name-server** statement, issue the following command at the **[edit]** level:

```
[edit]
user@host# protect groups test1 system name-server 10.1.2.1
user@host# protect groups test1 system name-server 10.1.2.4
```

**Results** Addresses 10.1.2.1 and 10.1.2.4 are protected.

## Unprotecting a Configuration

- Step-by-Step Procedure** Suppose you have the following configuration at the **[edit system]** hierarchy level:
- ```
protect: system {
  host-name bigping;
  domain-search 10.1.2.1;
  login {
    deny-sources {
      protect: address [ 172.17.28.19 172.17.28.173 172.17.28.0 174.0.0.0 ];
    }
  }
}
```
- To unprotect the entire **[edit system]** hierarchy level, issue the following command at the **[edit]** level:


```
[edit]
user@host# unprotect system
```
- Results** The entire **system** hierarchy level is unprotected.

Verification

Verify That a Hierarchy Is Protected Using the show Command

- Purpose** To check that a configuration hierarchy is protected.
- Action** In the configuration mode, issue the **show** command at the **[edit]** hierarchy level to see all the configuration hierarchies and configuration statements that are protected.



NOTE: All protected hierarchies or statements are prefixed with a **protect:** string.

```
...
protect: system {
  host-name bigping;
  domain-search 10.1.2.1;
  login {
    deny-sources {
      protect: address [ 172.17.28.19 172.17.28.173 172.17.28.0 174.0.0.0 ];
    }
  }
}
...
```

Verify That a Hierarchy Is Protected by Attempting to Modify a Configuration

- Purpose** To verify that a configuration is protected by trying to modify the configuration using the **activate**, **copy**, **insert**, **rename**, and **delete** commands.

Action To verify that a configuration is protected:

1. Try using the **activate**, **copy**, **insert**, **rename**, and **delete** commands for a top-level hierarchy or a child-level hierarchy or a statement within the hierarchy.

For a protected hierarchy or statement, the Junos OS displays an appropriate warning that the command has not executed. For example:

```
protect: system {
  host-name a;
  inactive: domain-search [ a b ];
}
```

2. To verify that the hierarchy is protected, try issuing the **activate** command for the **domain-search** statement:

```
[edit system]
```

```
user@host# activate system domain-search
```

The Junos OS CLI displays an appropriate message:

```
warning: [system] is protected, 'system domain-search' cannot be activated
```

Verify Usage of the protect Command

Purpose To view the **protect** commands used for protecting a configuration.

- Action**
1. Navigate to the required hierarchy.
 2. Issue the **show | display set relative** command.

```
user@host> show | display set relative
set system host-name bigping
set system domain-search 10.1.2.1
set system login deny-sources address 172.17.28.19
set system login deny-sources address 172.17.28.173
set system login deny-sources address 172.17.28.0
set system login deny-sources address 174.0.0.0
protect system login deny-sources address
protect system
```

View the Configuration in XML

Purpose To check if the protected hierarchies or statements are also displayed in the XML. Protected hierarchies, statements, or identifiers are displayed with the **| display xml** attribute in the XML.

Action To view the configuration in XML:

1. Navigate to the hierarchy you want to view and issue the **show** command with the pipe symbol and option **| display xml**:

[edit system]

```
user@host# show | display xml
[edit]
user@host# show system | display xml
<rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.2IO/junos">
  <configuration junos:changed-seconds="1291279234"
junos:changed-localtime="2010-12-02 00:40:34 PST">
    <system protect="protect">
      <host-name>bigping</host-name>
      <domain-search>10.1.2.1</domain-search>
      <login>
        <message>

          \jnpr

          \tUNAUTHORIZED USE OF THIS ROUTER
          \tIS STRICTLY PROHIBITED!

        </message>
        <class>
          <name>a</name>
          <allow-commands>commit-synchronize</allow-commands>
          <deny-commands>commit</deny-commands>
        </class>
        <deny-sources>
          <address protect="protect">172.17.28.19</address>
          <address protect="protect">172.17.28.173</address>
          <address protect="protect">172.17.28.0</address>
          <address protect="protect">174.0.0.0</address>
        </deny-sources>
      </login>
      <syslog>
        <archive>
        </archive>
      </syslog>
    </system>
  </configuration>
  <cli>
    <banner>[edit]</banner>
  </cli>
</rpc-reply>
```



NOTE: Loading an XML configuration with the `unprotect="unprotect"` tag unprotects an already protected hierarchy. For example, suppose you load the following XML hierarchy:

```
<protocols unprotect="unprotect">
  <ospf>
    <area>
      <name>0.0.0.0</name>
      <interface>
        <name>all</name>
      </interface>
```

```
</area>
</ospf>
</protocols>
```

The `[edit protocols]` hierarchy becomes unprotected if it is already protected.

Synchronizing Routing Engines

If your router has two Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the other by issuing the **commit synchronize** command. The Routing Engine on which you execute this command (requesting Routing Engine) copies and loads its candidate configuration to the other (responding Routing Engine). Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

The **commit synchronize** command does not work if the responding Routing Engine has uncommitted configuration changes. However, you can enforce commit synchronization on the Routing Engines by using the **force** option. When you issue the **commit synchronize** command with the **force** option from one Routing Engine, the configuration sessions on the other Routing Engine will be terminated and its configuration synchronized with that on the Routing Engine from which you issued the command.



NOTE: We recommend that you use the **force** option only if you are unable to resolve the issues that caused the **commit synchronize** command to fail.

For example, if you are logged in to **re1** (requesting Routing Engine) and you want **re0** (responding Routing Engine) to have the same configuration as **re1**, issue the **commit synchronize** command on **re1**. **re1** copies and loads its candidate configuration to **re0**. Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, **re1**'s candidate configuration is activated and becomes the current operational configuration on both Routing Engines.



NOTE: When you issue the **commit synchronize** command, you must use the groups **re0** and **re1**. For information about how to use the **apply-groups** statement, see [“Applying a Junos OS Configuration Group” on page 617](#).

The responding Routing Engine must be running Junos OS Release 5.0 or later.

To synchronize a Routing Engine's current operational configuration file with the other, log in to the Routing Engine from which you want to synchronize and issue the **commit synchronize** command:

```
[edit]
user@host# commit synchronize
commit complete
[edit]
user@host#
```



NOTE: You can also add the **commit synchronize** statement at the **[edit system]** hierarchy level so that a **commit** command automatically invokes a **commit synchronize** command by default. For more information, see the *Administration Guide for Security Devices*.

To enforce a **commit synchronize** on the Routing Engines, log in to the Routing Engine from which you want to synchronize and issue the **commit synchronize** command with the **force** option:

```
[edit]
user@host# commit synchronize force
re0:
re1:
commit complete
re0:
commit complete
[edit]
user@host#
```



NOTE:

- If you have nonstop routing enabled on your router, you must enter the **commit synchronize** command from the master Routing Engine after you make any changes to the configuration. If you enter this command on the backup Routing Engine, Junos OS displays a warning and commits the configuration.
- Starting with Junos OS Release 9.3, accounting of backup Routing Engine events or operations is not supported on accounting servers such as TACACS+ or RADIUS. Accounting is only supported for events or operations on a master Routing Engine.

For the **commit** synchronization process, the master Routing Engine commits the configuration and sends a copy of the configuration to the backup Routing Engine. Then the backup Routing Engine loads and commits the configuration. So, the **commit** synchronization between the master and backup Routing Engines takes place one Routing Engine at a time. If the configuration has a large text size or many **apply-groups**, **commit** times can be longer than desired.

You can use the **commit fast-synchronize** statement to have the synchronization between the master and backup Routing Engines occur simultaneously instead of sequentially. This can reduce the time needed for synchronization because the commits on the master and backup Routing Engines occur in parallel.

Include the **fast-synchronize** statement at the **[edit system]** hierarchy level to have synchronize occur simultaneously between the master and the backup Routing Engines:

```
[edit system]
commit fast-synchronize
```



NOTE:

- If commit fails on either Routing Engine, the commit process is rolled back on the other Routing Engine as well. This ensures that both Routing Engines have the same configuration.
- When the **fast-synchronize** statement is configured, the commits on the master Routing Engine and the backup Routing Engine run in parallel. In this process, the configuration is validated only on the Routing Engine where you execute the **commit** command. Therefore, it is recommended not to include too many configuration details in groups like **re0** and **re1**, because the configuration specified in group **re0** is applied only if the current Routing Engine is in slot 0. Likewise, the configuration specified in group **re1** is applied only if the current Routing Engine is in slot 1.
- Ensure that the Junos OS software version running on both the Routing Engines is the same.

**Related
Documentation**

- *Configuring the Junos OS to Support Redundancy on Routers Having Multiple Routing Engines or Switching Boards*
- *Junos OS Routing Engine Components and Processes*
- *Configuring Junos OS for the First Time on a Device with Dual Routing Engines*

Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically

If your router or switch has multiple Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the others by issuing the **commit synchronize** command.

To make the Routing Engines synchronize automatically whenever a configuration is committed, include the **commit synchronize** statement at the **[edit system]** hierarchy level:

```
[edit system]
commit synchronize;
```

The Routing Engine on which you execute the **commit** command (requesting Routing Engine) copies and loads its candidate configuration to the other (responding) Routing Engines. All Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on all Routing Engines.

For the commit synchronization process, the master Routing Engine commits the configuration and sends a copy of the configuration to the backup Routing Engine. Then the backup Routing Engine loads and commits the configuration. So, the commit synchronization between the master and backup Routing Engines takes place one Routing Engine at a time. If the configuration has a large text size or many apply-groups, commit times can be longer than desired.

You can use the **commit fast-synchronize** statement to have the synchronization between the master and backup Routing Engines occur simultaneously instead of sequentially. This can reduce the time needed for synchronization because the commits on the master and backup Routing Engines occur in parallel.

Include the **fast-synchronize** statement at the **[edit system]** hierarchy level to have synchronize occur simultaneously between the master and the backup Routing Engines:

```
[edit system]
commit fast-synchronize
```



NOTE:

- If commit fails on either Routing Engine, the commit process is rolled back on the other Routing Engine as well. This ensures that both Routing Engines have the same configuration.
- When the **fast-synchronize** statement is configured, the commits on the master Routing Engine and the backup Routing Engine run in parallel. In this process, the configuration is validated only on the Routing Engine where you execute the commit command. Therefore, it is recommended not to include too many configuration details in groups like **re0** and **re1**, because the configuration specified in group **re0** is applied only if the current Routing Engine is in slot 0. Likewise, the configuration specified in group **re1** is applied only if the current Routing Engine is in slot 1.
- Ensure that the Junos OS software version running on both the Routing Engines is same.

Related
Documentation

- [Junos OS Commit Model for Router or Switch Configuration on page 507](#)

CHAPTER 25

Using Operational Commands to Monitor a Device

- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)
- [Junos OS Operational Mode Commands That Combine Other Commands on page 566](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 567](#)
- [Controlling the Scope of an Operational Mode Command on page 568](#)
- [Monitoring Who Uses the Junos OS CLI on page 571](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 572](#)
- [Viewing Files and Directories on a Device Running Junos OS on page 573](#)
- [Displaying Junos OS Information on page 577](#)
- [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 579](#)
- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 584](#)
- [Example: Using Comments in Junos OS Operational Mode Commands on page 584](#)

Overview of Junos OS CLI Operational Mode Commands

This topic provides an overview of Junos OS CLI operational mode commands and contains the following sections:

- [CLI Command Categories on page 563](#)
- [Commonly Used Operational Mode Commands on page 565](#)

CLI Command Categories

When you log in to a device running Junos OS and the CLI starts, there are several broad groups of CLI commands:

- Commands for controlling the CLI environment—Some set commands in the **set** hierarchy configure the CLI display screen. For information about these commands, see [“Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies” on page 423](#).
- Commands for monitoring and troubleshooting—The following commands display information and statistics about the software and test network connectivity. Detailed command descriptions are provided in the *Junos OS Interfaces Command Reference*.
 - **clear**—Clear statistics and protocol database information.
 - **mtrace**—Trace mtrace packets from source to receiver.
 - **monitor**—Perform real-time debugging of various software components, including the routing protocols and interfaces.
 - **ping**—Determine the reachability of a remote network host.
 - **show**—Display the current configuration and information about interfaces, routing protocols, routing tables, routing policy filters, system alarms, and the chassis.
 - **test**—Test the configuration and application of policy filters and autonomous system (AS) path regular expressions.
 - **traceroute**—Trace the route to a remote network host.
- Commands for connecting to other network systems—The **ssh** command opens Secure Shell connections, and the **telnet** command opens telnet sessions to other hosts on the network. For information about these commands, see the [CLI Explorer](#).
- Commands for copying files—The **copy** command copies files from one location on the router or switch to another, from the router or switch to a remote system, or from a remote system to the router or switch. For information about these commands, see the [CLI Explorer](#).
- Commands for restarting software processes—The commands in the **restart** hierarchy restart the various Junos OS processes, including the routing protocol, interface, and SNMP. For information about these commands, see the [CLI Explorer](#).
- A command—**request**—for performing system-level operations, including stopping and rebooting the router or switch and loading Junos OS images. For information about this command, see the [CLI Explorer](#).
- A command—**start**—to exit the CLI and start a UNIX shell. For information about this command, see the [CLI Explorer](#).
- A command—**configure**—for entering configuration mode, which provides a series of commands that configure Junos OS, including the routing protocols, interfaces, network management, and user access. For information about the CLI configuration commands, see [“Understanding Junos OS CLI Configuration Mode” on page 456](#).
- A command—**quit**—to exit the CLI. For information about this command, see the [CLI Explorer](#).
- For more information about the CLI operational mode commands, see the [CLI Explorer](#).

Commonly Used Operational Mode Commands

Table 61 lists some operational commands you may find useful for monitoring router or switch operation. For a complete description of operational commands, see the Junos OS command references.



NOTE: The QFX3500 switch does not support the IS-IS, OSPF, BGP, MPLS, and RSVP protocols.

Table 61: Commonly Used Operational Mode Commands

Items to Check	Description	Command
Software version	Versions of software running on the router or switch	show version
Log files	Contents of the log files	monitor
	Log files and their contents and recent user logins	show log
Remote systems	Host reachability and network connectivity	ping
	Route to a network system	traceroute
Configuration	Current system configuration	show configuration
Manipulate files	List of files and directories on the router or switch	file list
	Contents of a file	file show
Interface information	Detailed information about interfaces	show interfaces
Chassis	Chassis alarm status	show chassis alarms
	Information currently on craft display	show chassis craft-interface
	Router or switch environment information	show chassis environment
	Hardware inventory	show chassis hardware
Routing table information	Information about entries in the routing tables	show route
Forwarding table information	Information about data in the kernel's forwarding table	show route forwarding-table
IS-IS	Adjacent routers or switches	show isis adjacency
OSPF	Display standard information about OSPF neighbors	show ospf neighbor
BGP	Display information about BGP neighbors	show bgp neighbor

Table 61: Commonly Used Operational Mode Commands (*continued*)

Items to Check	Description	Command
MPLS	Status of interfaces on which MPLS is running	show mpls interface
	Configured LSPs on the router or switch, as well as all ingress, transit, and egress LSPs	show mpls lsp
	Routes that form a label-switched path	show route label-switched-path
RSVP	Status of interfaces on which RSVP is running	show rsvp interface
	Currently active RSVP sessions	show rsvp session
	RSVP packet and error counters	show rsvp statistics

**Related
Documentation**

- [Junos OS Operational Mode Commands That Combine Other Commands on page 566](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 567](#)

Junos OS Operational Mode Commands That Combine Other Commands

In some cases, some Junos OS operational commands are created from a combination of other operational commands. These commands can be useful shortcuts for collecting information about the device, as shown in [Figure 20](#).

Figure 20: Commands That Combine Other Commands

The **request support information** command provides output from a combination of other operational commands.

```

user@host> request support information

root@host> show system uptime

Current time: 2007-02-16 13:10:08 PST
System booted: 2007-02-02 09:21:50 PST (2w0d 03:48 ago)
Protocols started: 2007-02-02 09:24:42 PST (2w0d 03:45 ago)
Last configured: 2007-02-16 03:04:58 PST (10:05:10 ago) by root
1:10PM up 14 days, 3:48, 2 users, load averages: 0.01, 0.02, 0.00

root@host> show version detail

Hostname: host
Model: m320
JUNOS Base OS boot [8.3-R1.1]

root@host> show system core-dumps

/var/tmp/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory

/var/crash/cores:
total 9780
-rw-r--r-- 1 root wheel 4990976 Feb 9 15:39
core-FPC2.core.0.060209.1539

root@host> show chassis hardware detail

Hardware inventory:
Item          Version  Part number  Serial number  Description
Chassis
Backplane     REV 07   710-001517   AW44 31       M20 Backplane
Power Supply B REV 09   740-001466   0042 33       DC Power Supply

```

Related Documentation

- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 567](#)

Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands

The Junos OS operational mode commands can include **brief**, **detail**, **extensive**, or **terse** options. You can use these options to control the amount of information you want to view.

1. Use the **?** prompt to list options available for the command. For example:

```

user@host> show interfaces fe-1/1/1 ?
Possible completions:
<[Enter]>      Execute this command
brief          Display brief output
descriptions   Display interface description strings
detail         Display detailed output
extensive      Display extensive output
media          Display media information
snmp-index     SNMP index of interface
statistics     Display statistics and detailed output
terse          Display terse output
|              Pipe through a command

```

2. Choose the option you wish to use with the command. (See [Figure 21.](#))

Figure 21: Command Output Options

Command output with the **brief** option.

```

user@host> show interfaces fe-1/1/1 brief
Physical interface: fe-1/1/1, Enabled, Physical link is Down
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback:
Disabled, Source filtering: Disabled,
Flow control: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
Link flags : None

```

Command output with the **terse** option.

```

user@host> show interfaces fe-1/1/1 terse
Interface      Admin Link Proto  Local      Remote
fe-1/1/1       up      down

```

Command output with the **extensive** option.

```

user@host> show interfaces fe-1/1/1 extensive
Physical interface: fe-1/1/1, Enabled, Physical link is Down
Interface index: 141, SNMP ifIndex: 33, Generation: 24
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback:
Disabled, Source filtering: Disabled,
Flow control: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 4 supported, 4 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:90:69:d0:f8:9e, Hardware address: 00:90:69:d0:f8:9e
Last flapped : 2007-02-02 09:26:25 PST (2w0d 03:40 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes :                0                0 bps
Output bytes :                0                0 bps
Input packets:                0                0 pps
Output packets:              0                0 pps
--(more)--

```

Related Documentation

- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)
- [Controlling the Scope of an Operational Mode Command on page 568](#)

Controlling the Scope of an Operational Mode Command

The Junos OS CLI operational commands include options that you can use to identify specific components on a device running Junos OS. For example:

1. Type the **show interfaces** command to display information about all interfaces on the router.

```

user@host> show interfaces
Physical interface: so-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 23
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 13861 (00:00:05 ago), Output: 13891 (00:00:01 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mppls:
Not-configured
CHAP state: Closed
PAP state: Closed

```



```

CoS queues      : 4 supported, 4 maximum usable queues
Last flapped    : 2008-06-02 17:16:14 PDT (1d 14:21 ago)
Input rate      : 40 bps (0 pps)
Output rate     : 48 bps (0 pps)

```

---(more)---

2. To display information about a specific interface, type that interface as a command option:

```

user@host> show interfaces fe-0/1/3
Physical interface: fe-0/1/3, Enabled, Physical link is Up
  Interface index: 135, SNMP ifIndex: 30
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, MAC-REWRITE Error:
None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 4 supported, 4 maximum usable queues
  Current address: 00:05:85:8f:c8:22, Hardware address: 00:05:85:8f:c8:22
  Last flapped   : 2008-06-02 17:16:15 PDT (1d 14:28 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None

user@host>

```

Operational Mode Commands on a TX Matrix Router or TX Matrix Plus Router

When you issue operational mode commands on the TX Matrix router, CLI command options allow you to restrict the command output to show only a component of the routing matrix rather than the routing matrix as a whole.

These are the options shown in the CLI:

- **scc**—The TX Matrix router (or switch-card chassis)
- **sfc**—The TX Matrix Plus router (also referred to as or switch-fabric chassis)
- **lcc number**—A specific router in a routing matrix based on a TX Matrix router or a TX Matrix Plus router.
- **all-lcc**—All T640 routers (in a routing matrix based on a TX Matrix router) or all T1600 routers or T4000 routers (in a routing matrix based on a TX Matrix Plus router).

If you specify none of these options, then the command applies by default to the whole routing matrix.

Examples of Routing Matrix Command Options

The following output samples, using the **show version** command, demonstrate some different options for viewing information about the routing matrix.

```

user@host> show version ?
Possible completions:
  <[Enter]>      Execute this command
  all-lcc       Show software version on all LCC chassis

```

brief	Display brief output
detail	Display detailed output
lcc	Show software version on specific LCC (0..3)
scc	Show software version on the SCC
	Pipe through a command

Sample Output: No Routing Matrix Options Specified

```

user@host> show version
scc-re0:
-----
Hostname: scc
Model: TX Matrix
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
lcc0-re0:
-----
Hostname: lcc0
Model: t640
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
JUNOS Support Tools Package [7.0-20040630.0]
lcc1-re0:
-----
Hostname: lcc1
Model: t640
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
JUNOS Support Tools Package [7.0-20040630.0]

```

Sample Output: TX Matrix Router Only (scc Option)

```

user@host> show version scc
Hostname: scc
Model: TX Matrix
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]

```

Sample Output: Specific T640 Router (lcc number Option)

```

user@host> show version lcc 0

```

```
lcc0-re0:
```

```
-----
Hostname: lcc0
Model: t640
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
JUNOS Support Tools Package [7.0-20040630.0]
```

Sample Output: All T640 Routers (all-lcc Option)

```
user@host> show version all-lcc
lcc0-re0:
```

```
-----
Hostname: lcc0
Model: t640
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
JUNOS Support Tools Package [7.0-20040630.0]
lcc1-re0:
```

```
-----
Hostname: lcc1
Model: t640
JUNOS Base OS boot [7.0-20040630.0]
JUNOS Base OS Software Suite [7.0-20040629.0]
JUNOS Kernel Software Suite [7.0-20040630.0]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0-20040630.0]
JUNOS Routing Software Suite [7.0-20040630.0]
JUNOS Online Documentation [7.0-20040630.0]
JUNOS Crypto Software Suite [7.0-20040630.0]
JUNOS Support Tools Package [7.0-20040630.0]
```

- Related Documentation**
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 572](#)
 - [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 584](#)

Monitoring Who Uses the Junos OS CLI

Depending upon how you configure Junos OS, multiple users can log in to the router, use the CLI, and configure or modify the software configuration.

If, when you enter configuration mode, another user is also in configuration mode, a notification message is displayed that indicates who the user is and what portion of the configuration the person is viewing or editing:

```
user@host> configure
Entering configuration mode
```

```
Users currently editing the configuration:
  root terminal d0 (pid 4137) on since 2008-04-09 23:03:07 PDT, idle 7w6d 08:22
    [edit]
The configuration has been changed but not committed

[edit]
user@host#
```

**Related
Documentation**

- [Entering and Exiting the Junos OS CLI Configuration Mode on page 462](#)
- [Controlling the Junos OS CLI Environment on page 645](#)

Interface Naming Conventions Used in the Junos OS Operational Commands

This topic explains the interface naming conventions used in the Junos OS operational commands, and contains the following sections:

- [Physical Part of an Interface Name on page 572](#)
- [Logical Part of an Interface Name on page 572](#)
- [Channel Identifier Part of an Interface Name on page 573](#)

Physical Part of an Interface Name

The physical interface naming conventions for Junos OS platforms is as follows:

- On SRX devices, the unique name of each network interface has the following format to identify the physical device that corresponds to a single physical network connector:

type-slot/pim-or-ioc/port

- On other platforms, when you display information about an interface, you specify the interface type, the slot in which the Flexible PIC Concentrator (FPC) is installed, the slot on the FPC in which the PIC is located, and the configured port number.

In the physical part of the interface name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers:

type-fpc/pic/port



NOTE: Exceptions to the ***type-fpc/pic/port*** physical description include the aggregated Ethernet and aggregated SONET/SDH interfaces, which use the syntax ***aenumber*** and ***asnumber***, respectively.

Logical Part of an Interface Name

The logical unit part of the interface name corresponds to the logical unit number, which can be a number from 0 through 16,384. In the virtual part of the name, a period (.) separates the port and logical unit numbers:

- SRX devices:

type-slot/pim-or-ioc/port:channel.unit

- Other platforms:

type-fpc/pic/port.logical

Channel Identifier Part of an Interface Name

The channel identifier part of the interface name is required only on channelized interfaces. For channelized interfaces, channel 0 identifies the first channelized interface. For channelized intelligent queuing (IQ) interfaces, channel 1 identifies the first channelized interface.



NOTE: Depending on the type of channelized interface, up to three levels of channelization can be specified. For more information, see the *Junos Network Interfaces Configuration Guide*.

A colon (:) separates the physical and virtual parts of the interface name:

- SRX devices:

type-slot/pim-or-ioc/port:channel
type-slot/pim-or-ioc/port:channel:channel
type-slot/pim-or-ioc/port:channel:channel:channel

- Other platforms:

type-fpc/pic/port:channel
type-fpc//pic/port:channel:channel
type-fpc/pic/port:channel:channel:channel

Related Documentation

- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 626](#)
- [Junos OS Network Interfaces Library for Routing Devices](#)

Viewing Files and Directories on a Device Running Junos OS

Junos OS stores information in files on the device, including configuration files, log files, and router software files. This topic shows some examples of operational commands that you can use to view files and directories on a device running Junos OS.

Sections include:

- [Directories on the Router or Switch on page 573](#)
- [Listing Files and Directories on page 574](#)
- [Specifying Filenames and URLs on page 576](#)

Directories on the Router or Switch

Table 62 lists some standard directories on a device running Junos OS.

Table 62: Directories on the Router

Directory	Description
<code>/config</code>	This directory is located on the device's router's internal flash drive. It contains the active configuration (juniper.conf) and rollback files 1, 2, and 3.
<code>/var/db/config</code>	This directory is located on the router's device's hard drive and contains rollback files 4 through 49.
<code>/var/tmp</code>	This directory is located on the device's hard drive. It holds core files from the various processes on the Routing Engines. Core files are generated when a particular process crashes and are used by Juniper Networks engineers to diagnose the reason for failure.
<code>/var/log</code>	This directory is located on the device's hard drive. It contains files generated by both the device's logging function as well as the traceoptions command.
<code>/var/home</code>	This directory is located on the device's hard drive. It contains a subdirectory for each configured user on the device. These individual user directories are the default file location for many Junos OS commands.
<code>/altroot</code>	This directory is located on the device's hard drive and contains a copy of the root file structure from the internal flash drive. This directory is used in certain disaster recovery modes where the internal flash drive is not operational.
<code>/altconfig</code>	This directory is located on the device's hard drive and contains a copy of the <code>/config</code> file structure from the internal flash drive. This directory is also used in certain disaster recovery modes when the internal flash drive is not operational.

Listing Files and Directories

You can view the device's directory structure as well as individual files by issuing the **file** command in operational mode.

- To get help about the **file** command, type the following:

```

user@host> file ?
Possible completions:
<[Enter]>      Execute this command
archive       Archives files from the system
checksum      Calculate file checksum
compare       Compare files
copy          Copy files (local or remote)
delete        Delete files from the system
list          List file information
rename        Rename files
show          Show file contents
source-address Local address to use in originating the connection
|            Pipe through a command
user@host> file

```

Help shows that the **file** command includes several options for manipulating files.

2. Use the **list** option to see the directory structure of the device. For example, to show the files located in your home directory on the device:

```
user@host> file list
.ssh/
common
```

The default directory for the **file list** command is the home directory of the user logged in to the device. In fact, the user's home directory is the default directory for most of Junos OS commands requiring a filename.

3. To view the contents of other file directories, specify the directory location. For example:

```
user@host> file list /config
juniper.conf
juniper.conf.1.gz
juniper.conf.2.gz
juniper.conf.3.gz
```

4. You can also use the device's context-sensitive help system to locate a directory. For example:

```
user@host> file list /?
Possible completions:
<[Enter]>      Execute this command
<path>        Path to list
/COPYRIGHT     Size: 6355, Last changed: Feb 13 2005
/altconfig/    Last changed: Aug 07 2007
/altroot/      Last changed: Aug 07 2007
/bin/          Last changed: Apr 09 22:31:35
/boot/         Last changed: Apr 09 23:28:39
/config/       Last changed: Apr 16 22:35:35
/data/         Last changed: Aug 07 2007
/dev/          Last changed: Apr 09 22:36:21
/etc/          Last changed: Apr 11 03:14:22
/kernel        Size: 27823246, Last changed: Aug 07 2007
/mfs/          Last changed: Apr 09 22:36:49
/mnt/          Last changed: Jan 11 2007
/modules/      Last changed: Apr 09 22:33:54
/opt/          Last changed: Apr 09 22:31:00
/packages/     Last changed: Apr 09 22:34:38
/proc/         Last changed: May 07 20:25:46
/rdm.taf       Size: 498, Last changed: Apr 09 22:37:31
/root/         Last changed: Apr 10 02:19:45
/sbin/         Last changed: Apr 09 22:33:55
/staging/      Last changed: Apr 09 23:28:41
/tmp/          Last changed: Apr 11 03:14:49
/usr/          Last changed: Apr 09 22:31:34
/var/          Last changed: Apr 09 22:37:30
user@host> file list /var/?
<[Enter]>      Execute this command
<path>        Path to list
/var/account/  Last changed: Jul 09 2007
/var/at/       Last changed: Jul 09 2007
/var/backups/  Last changed: Jul 09 2007
/var/bin/      Last changed: Jul 09 2007
/var/crash/    Last changed: Apr 09 22:31:08
/var/cron/     Last changed: Jul 09 2007
```

```

/var/db/                Last changed: May 07 20:28:40
/var/empty/             Last changed: Jul 09 2007
/var/etc/               Last changed: Apr 16 22:35:36
/var/heimdal/           Last changed: Jul 10 2007
/var/home/              Last changed: Apr 09 22:59:18
/var/jail/              Last changed: Oct 31 2007
/var/log/               Last changed: Apr 17 02:00:10
/var/mail/              Last changed: Jul 09 2007
/var/messages/          Last changed: Jul 09 2007
/var/named/             Last changed: Jul 10 2007
/var/packages/          Last changed: Jan 18 02:38:59
/var/pdb/               Last changed: Oct 31 2007
/var/preserve/          Last changed: Jul 09 2007
/var/run/               Last changed: Apr 17 02:00:01
/var/rundb/             Last changed: Apr 17 00:46:00
/var/rwho/              Last changed: Jul 09 2007
/var/sdb/               Last changed: Apr 09 22:37:31
/var/spool/             Last changed: Jul 09 2007
/var/sw/                Last changed: Jul 09 2007
/var/tmp/               Last changed: Apr 09 23:28:41
/var/transfer/          Last changed: Jul 09 2007
/var/yp/                Last changed: Jul 09 2007
user@host> file list /var/

```

5. You can also display the contents of a file. For example:

```

user@host>file show /var/log/inventory
Jul  9 23:17:46 CHASSISD release 8.4I0 built by builder on 2007-06-12 07:58:27
UTC
Jul  9 23:18:05 CHASSISD release 8.4I0 built by builder on 2007-06-12 07:58:27
UTC
Jul  9 23:18:06 Routing Engine 0 - part number 740-003239, serial number
9000016755
Jul  9 23:18:15 Routing Engine 1 - part number 740-003239, serial number
9001018324
Jul  9 23:19:03 SSB 0 - part number 710-001951, serial number AZ8025
Jul  9 23:19:03 SSRAM bank 0 - part number 710-001385, serial number 243071
Jul  9 23:19:03 SSRAM bank 1 - part number 710-001385, serial number 410608
...

```

Specifying Filenames and URLs

In some CLI commands and configuration statements—including **file copy**, **file archive**, **load**, **save**, **set system login user *username* authentication *load-key-file***, and **request system software add**—you can include a filename. On a routing matrix, you can include chassis information as part of the filename (for example, **lcc0**, **lcc0-re0**, or **lcc0-re1**).

You can specify a filename or URL in one of the following ways:

- **filename**—File in the user's current directory on the local flash drive. You can use wildcards to specify multiple source files or a single destination file. Wildcards are not supported in Hypertext Transfer Protocol (HTTP) or FTP.



NOTE: Wildcards are supported only by the **file** (**compare** | **copy** | **delete** | **list** | **rename** | **show**) commands. When you issue the **file show** command with a wildcard, it must resolve to one filename.

- **path/filename**—File on the local flash disk.
- **/var/filename** or **/var/path/filename**—File on the local hard disk. You can also specify a file on a local Routing Engine for a specific T640 router on a routing matrix:

```
user@host> file delete lcc0-re0:/var/tmp/junk
```
- **a:filename** or **a:path/filename**—File on the local drive. The default path is / (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.
- **hostname:/path/filename**, **hostname:filename**, **hostname:path/filename**, or **scp://hostname/path/filename**—File on an scp/ssh client. This form is not available in the worldwide version of Junos OS. The default path is the user's home directory on the remote system. You can also specify **hostname** as **username@hostname**.
- **ftp://hostname/path/filename**—File on an FTP server. You can also specify **hostname** as **username@hostname** or **username:password@hostname**. The default path is the user's home directory. To specify an absolute path, the path must start with **%2F**; for example, **ftp://hostname/%2Fpath/filename**. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required, and you do not specify the password or **prompt**, an error message is displayed:

```
user@host> file copy ftp://username@ftp.hostname.net//filename
file copy ftp.hostname.net: Not logged in.

user@host> file copy ftp://username:prompt@ftp.hostname.net//filename
Password for username@ftp.hostname.net:
```
- **http://hostname/path/filename**—File on an HTTP server. You can also specify **hostname** as **username@hostname** or **username:password@hostname**. If a password is required and you omit it, you are prompted for it.
- **re0:/path/filename** or **re1:/path/filename**—File on a local Routing Engine. You can also specify a file on a local Routing Engine for a specific T640 router on a routing matrix:

```
user@host> show log lcc0-re1:chassisd
```

Related
Documentation

- [Displaying Junos OS Information on page 577](#)

Displaying Junos OS Information

You can display Junos OS version information and other status to determine if the version of Junos OS that you are running supports particular features or hardware.

To display Junos OS information:

1. Make sure you are in operational mode.
2. To display brief information and status for the kernel and Packet Forwarding Engine, enter the **show version brief** command. This command shows version information for Junos OS packages installed on the router. For example:

```
user@host> show version brief
Hostname: host
Model: m7i
JUNOS Base OS boot [9.1R1.8]
JUNOS Base OS Software Suite [9.1R1.8]
JUNOS Kernel Software Suite [9.1R1.8]
JUNOS Crypto Software Suite [9.1R1.8]
JUNOS Packet Forwarding Engine Support (M/T Common) [9.1R1.8]
JUNOS Packet Forwarding Engine Support (M7i/M10i) [9.1R1.8]
JUNOS Online Documentation [9.1R1.8]
JUNOS Routing Software Suite [9.1R1.8]
```

```
user@host>
```

If the **Junos Crypto Software Suite** is listed, the router has Canada and USA encrypted Junos OS. If the **Junos Crypto Software Suite** is not listed, the router is running worldwide nonencrypted Junos OS.

3. To display detailed version information, enter the **show version detail** command. This command display shows the hostname and version information for Junos OS packages installed on your router. It also includes the version information for each software process. For example:

```
user@host> show version detail

Hostname: host
Model: m20
JUNOS Base OS boot [8.4R1.13]
JUNOS Base OS Software Suite [8.4R1.13]
JUNOS Kernel Software Suite [8.4R1.13]
JUNOS Crypto Software Suite [8.4R1.13]
JUNOS Packet Forwarding Engine Support (M/T Common) [8.4R1.13]
JUNOS Packet Forwarding Engine Support (M20/M40) [8.4R1.13]
JUNOS Online Documentation [8.4R1.13]
JUNOS Routing Software Suite [8.4R1.13]
KERNEL 8.4R1.13 #0 built by builder on 2007-08-08 00:33:41 UTC
MGD release 8.4R1.13 built by builder on 2007-08-08 00:34:00 UTC
CLI release 8.4R1.13 built by builder on 2007-08-08 00:34:47 UTC
RPD release 8.4R1.13 built by builder on 2007-08-08 00:45:21 UTC
CHASSISD release 8.4R1.13 built by builder on 2007-08-08 00:36:59 UTC
DFWD release 8.4R1.13 built by builder on 2007-08-08 00:39:32 UTC
DCD release 8.4R1.13 built by builder on 2007-08-08 00:34:24 UTC
SNMPD release 8.4R1.13 built by builder on 2007-08-08 00:42:24 UTC
MIB2D release 8.4R1.13 built by builder on 2007-08-08 00:46:47 UTC
APSD release 8.4R1.13 built by builder on 2007-08-08 00:36:39 UTC
VRRPD release 8.4R1.13 built by builder on 2007-08-08 00:45:44 UTC
ALARM release 8.4R1.13 built by builder on 2007-08-08 00:34:30 UTC
PFED release 8.4R1.13 built by builder on 2007-08-08 00:41:54 UTC
CRAFTD release 8.4R1.13 built by builder on 2007-08-08 00:39:03 UTC
SAMPLED release 8.4R1.13 built by builder on 2007-08-08 00:36:05 UTC
ILMID release 8.4R1.13 built by builder on 2007-08-08 00:36:51 UTC
RMOPD release 8.4R1.13 built by builder on 2007-08-08 00:42:04 UTC
```

```

COSD release 8.4R1.13 built by builder on 2007-08-08 00:38:39 UTC
FSAD release 8.4R1.13 built by builder on 2007-08-08 00:43:01 UTC
IRSD release 8.4R1.13 built by builder on 2007-08-08 00:35:37 UTC
FUD release 8.4R1.13 built by builder on 2007-08-08 00:44:36 UTC
RTSPD release 8.4R1.13 built by builder on 2007-08-08 00:29:14 UTC
SMARTD release 8.4R1.13 built by builder on 2007-08-08 00:13:32 UTC
KSYNCD release 8.4R1.13 built by builder on 2007-08-08 00:33:17 UTC
SPD release 8.4R1.13 built by builder on 2007-08-08 00:43:50 UTC
L2TPD release 8.4R1.13 built by builder on 2007-08-08 00:43:12 UTC
HTTPD release 8.4R1.13 built by builder on 2007-08-08 00:36:27 UTC
PPPOED release 8.4R1.13 built by builder on 2007-08-08 00:36:04 UTC
RDD release 8.4R1.13 built by builder on 2007-08-08 00:33:49 UTC
PPPD release 8.4R1.13 built by builder on 2007-08-08 00:45:13 UTC
DFCD release 8.4R1.13 built by builder on 2007-08-08 00:39:11 UTC
DLSWD release 8.4R1.13 built by builder on 2007-08-08 00:42:37 UTC
LACPD release 8.4R1.13 built by builder on 2007-08-08 00:35:41 UTC
USBD release 8.4R1.13 built by builder on 2007-08-08 00:30:01 UTC
LFMD release 8.4R1.13 built by builder on 2007-08-08 00:35:52 UTC
CFMD release 8.4R1.13 built by builder on 2007-08-08 00:34:45 UTC
JDHCPD release 8.4R1.13 built by builder on 2007-08-08 00:35:40 UTC
PGCPD release 8.4R1.13 built by builder on 2007-08-08 00:46:31 UTC
SSD release 8.4R1.13 built by builder on 2007-08-08 00:36:17 UTC
MSPD release 8.4R1.13 built by builder on 2007-08-08 00:33:42 UTC
KMD release 8.4R1.13 built by builder on 2007-08-08 00:44:02 UTC
PPMD release 8.4R1.13 built by builder on 2007-08-08 00:36:03 UTC
LMPD release 8.4R1.13 built by builder on 2007-08-08 00:33:49 UTC
LRMUXD release 8.4R1.13 built by builder on 2007-08-08 00:33:55 UTC
PGMD release 8.4R1.13 built by builder on 2007-08-08 00:36:01 UTC
BFDD release 8.4R1.13 built by builder on 2007-08-08 00:44:22 UTC
SDXD release 8.4R1.13 built by builder on 2007-08-08 00:36:18 UTC
AUDITD release 8.4R1.13 built by builder on 2007-08-08 00:34:40 UTC
L2ALD release 8.4R1.13 built by builder on 2007-08-08 00:40:05 UTC
EVENTD release 8.4R1.13 built by builder on 2007-08-08 00:39:55 UTC
L2CPD release 8.4R1.13 built by builder on 2007-08-08 00:41:04 UTC
MPLSOAMD release 8.4R1.13 built by builder on 2007-08-08 00:45:11 UTC
jroute-dd release 8.4R1.13 built by builder on 2007-08-08 00:31:01 UTC
jkernel-dd release 8.4R1.13 built by builder on 2007-08-08 00:30:30 UTC
jcrypto-dd release 8.4R1.13 built by builder on 2007-08-08 00:30:12 UTC
jdocs-dd release 8.4R1.13 built by builder on 2007-08-08 00:02:52 UTC

```

user@host>

Related Documentation • [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 579](#)

Managing Programs and Processes Using Junos OS Operational Mode Commands

This topic shows some examples of Junos operational commands that you can use to manage programs and processes on a device running Junos OS.

Sections include:

- [Showing Software Processes on page 580](#)
- [Restarting the Junos OS Process on page 581](#)
- [Stopping Junos OS on page 582](#)
- [Rebooting Junos OS on page 583](#)

Showing Software Processes

To verify system operation or to begin diagnosing an error condition, you may need to display information about software processes running on the device.

To show software processes:

1. Make sure you are in operational mode.
2. Type the **show system processes extensive** command. This command shows the CPU utilization on the device and lists the processes in order of CPU utilization. For example:

```
user@host> show system processes extensive
```

```
Last pid: 28689; load averages: 0.01, 0.00, 0.00 up 56+06:16:13 04:52:04
73 processes: 1 running, 72 sleeping
```

```
Mem: 101M Active, 101M Inact, 98M Wired, 159M Cache, 69M Buf, 286M Free
Swap: 1536M Total, 1536M Free
```

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
3365	root	2	0	21408K	4464K	select	511:23	0.00%	0.00%	chassisd
3508	root	2	0	3352K	1168K	select	32:45	0.00%	0.00%	l2ald
3525	root	2	0	3904K	1620K	select	13:40	0.00%	0.00%	dcd
5532	root	2	0	11660K	2856K	kqread	10:36	0.00%	0.00%	rpd
3366	root	2	0	2080K	828K	select	8:33	0.00%	0.00%	alarmd
3529	root	2	0	2040K	428K	select	7:32	0.00%	0.00%	irsd
3375	root	2	0	2900K	1600K	select	6:01	0.00%	0.00%	ppmd
3506	root	2	0	5176K	2568K	select	5:38	0.00%	0.00%	mib2d
4957	root	2	0	1284K	624K	select	5:16	0.00%	0.00%	ntpd
6	root	18	0	0K	0K	syncer	4:49	0.00%	0.00%	syncer
3521	root	2	0	2312K	928K	select	2:14	0.00%	0.00%	lfmd
3526	root	2	0	5192K	1988K	select	2:04	0.00%	0.00%	snmpd
3543	root	2	0	0K	0K	peer_s	1:46	0.00%	0.00%	peer proxy
3512	root	2	0	3472K	1044K	select	1:44	0.00%	0.00%	rmopd
3537	root	2	0	0K	0K	peer_s	1:30	0.00%	0.00%	peer proxy
3527	root	2	0	3100K	1176K	select	1:14	0.00%	0.00%	pfed
3380	root	2	0	3208K	1052K	select	1:11	0.00%	0.00%	bfdd
4136	root	2	0	11252K	3668K	select	0:54	0.00%	0.00%	cli
3280	root	2	0	2248K	1420K	select	0:28	0.00%	0.00%	eventd
3528	root	2	0	2708K	672K	select	0:28	0.00%	0.00%	dfwd
7	root	-2	0	0K	0K	vlruwt	0:26	0.00%	0.00%	vnlr
3371	root	2	0	1024K	216K	sbwait	0:25	0.00%	0.00%	tnp.snmpd
13	root	-18	0	0K	0K	psleep	0:24	0.00%	0.00%	vmuncacheda
3376	root	2	0	1228K	672K	select	0:22	0.00%	0.00%	smartd
5	root	-18	0	0K	0K	psleep	0:17	0.00%	0.00%	bufdaemon
3368	root	2	0	15648K	9428K	select	0:17	0.00%	0.00%	mgd
3362	root	2	0	1020K	204K	select	0:15	0.00%	0.00%	watchdog
3381	root	2	0	2124K	808K	select	0:15	0.00%	0.00%	lacpd
3524	root	2	0	6276K	1492K	select	0:14	0.00%	0.00%	kmd
3343	root	10	0	1156K	404K	nanslp	0:14	0.00%	0.00%	cron

---(more)---

Table 63 lists and describes the output fields included in this example. The fields are listed in alphabetical order.

Table 63: show system process extensive Command Output Fields

Field	Description
COMMAND	Command that is running.
CPU	Raw (unweighted) CPU usage. The value of this field is used to sort the processes in the output.
last pid	Last process identifier assigned to the process.
load averages	Three load averages, followed by the current time.
Mem	Information about physical and virtual memory allocation.
NICE	UNIX “nice” value. The nice value allows a process to change its final scheduling priority.
PID	Process identifier.
PRI	Current kernel scheduling priority of the process. A lower number indicates a higher priority.
processes	Number of existing processes and the number of processes in each state (sleeping , running , starting , zombies , and stopped).
RES	Current amount of resident memory, in KB.
SIZE	Total size of the process (text , data , and stack), in KB.
STATE	Current state of the process (sleep , wait , run , idle , zombi , or stop).
Swap	Information about physical and virtual memory allocation.
USERNAME	Owner of the process.
WCPU	Weighted CPU usage.

Restarting the Junos OS Process

To correct an error condition, you might need to restart a software process running on the device. You can use the **restart** command to force a restart of a software process.



CAUTION: Do not restart a software process unless specifically asked to do so by your Juniper Networks customer support representative. Restarting a software process during normal operation of a device could cause interruption of packet forwarding and loss of data.

To restart a software process:

1. Make sure you are in operational mode.
2. Type the following command:

```
user@host> restart process-name < (immediately | gracefully | soft) >
```

- **process-name** is the name of the process that you want to restart. For example, **routing** or **class-of-service**. You can use the command completion feature of Junos OS to see a list of software processes that you can restart using this command.
- **gracefully** restarts the software process after performing clean-up tasks.
- **immediately** restarts the software process without performing any clean-up tasks.
- **soft** rereads and reactivates the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant.

The following example shows how to restart the routing process:

```
user@host> restart routing
Routing protocol daemon started, pid 751
```

When a process restarts, the process identifier (PID) is updated. (See [Figure 22](#).)

Figure 22: Restarting a Process

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
546	root	10	0	9096K	1720K	nanslp	0:21	0.00%	0.00%	chassisd
685	root	2	0	12716K	3840K	kqread	0:01	0.00%	0.00%	rpdp
553	root	2	0	8792K	1544K	select	0:01	0.00%	0.00%	mib2d

PID before restart

547	root	2	0	7732K	888K	select	0:00	0.00%	0.00%	alarmd
545	root	2	0	10292K	2268K	select	0:00	0.00%	0.00%	dcd
1	root	10	0	816K	520K	wait	0:00	0.00%	0.00%	init
550	root	2	-12	1308K	692K	select	0:00	0.00%	0.00%	ntpd
758	root	32	0	21716K	832K	RUN	0:00	0.00%	0.00%	top
560	root	2	0	8208K	1088K	select	0:00	0.00%	0.00%	rmopd
561	root	2	0	8188K	1156K	select	0:00	0.00%	0.00%	cosd
559	root	2	0	1632K	840K	select	0:00	0.00%	0.00%	ilmid
573	lab	2	0	7480K	2580K	select	0:00	0.00%	0.00%	cli
751	root	2	0	12716K	3944K	kqread	0:00	0.00%	0.00%	rpdp
558	root	2	20	8708K	1880K	select	0:00	0.00%	0.00%	sampld
555	root	2	0	1856K	932K	select	0:00	0.00%	0.00%	vrpd
686	root	2	0	7808K	940K	select	0:00	0.00%	0.00%	apsd

PID after restart

Stopping Junos OS

To avoid damage to the file system and to prevent loss of data, you must always gracefully shut down Junos OS before powering off the device.



NOTE: SRX Series Services Gateway devices for the branch and EX Series Ethernet Switches support resilient dual-root partitioning.

If you are unable to shut down a device gracefully because of unexpected circumstances such as a power outage or a device failure, resilient dual-root partitioning prevents file corruption and enables a device to remain operational. In addition, it enables a device to boot transparently from the second root partition if the system fails to boot from the primary root partition.

Resilient dual-root partitioning serves as a backup mechanism for providing additional resiliency to a device when there is an abnormal shutdown. However, it is not an alternative to performing a graceful shutdown under normal circumstances.

To stop Junos OS:

1. Make sure you are in operational mode.
2. Enter the **request system halt** command. This command stops all system processes and halts the operating system. For example:

```
user@host> request system halt
Halt the system? [yes,no] (no) yes
shutdown: [pid 3110]
Shutdown NOW!
*** FINAL System shutdown message from root@host ***
System going down IMMEDIATELY
user@host> Dec 17 17:28:40 init: syslogd (PID 2514) exited with status=0 Normal
Exit
Waiting (max 60 seconds) for system process `bufdaemon' to stop...stopped
Waiting (max 60 seconds) for system process `syncer' to stop...stopped
syncing disks... 4
done
Uptime: 3h31m41s
ata0: resetting devices.. done
The operating system has halted.
Please press any key to reboot.
```

Rebooting Junos OS

After a software upgrade or to recover (occasionally) from an error condition, you must reboot Junos OS.

To reboot Junos OS:

1. Make sure you are in operational mode.
2. Enter the **request system reboot** command. This command displays the final stages of the system shutdown and executes the reboot. Reboot requests are recorded to the system log files, which you can view with the **show log messages** command. For example:

```
user@host> request system reboot
Reboot the system? [yes,no] (no) yes
```

```
shutdown: [pid 845]
Shutdown NOW!
*** FINAL System shutdown message from root@host ***
System going down IMMEDIATELY
user@host> Dec 17 17:34:20 init: syslogd (PID 409) exited with status=0 Normal
Exit
Waiting (max 60 seconds) for system process `bufdaemon' to stop...stopped
Waiting (max 60 seconds) for system process `syncer' to stop...stopped
syncing disks... 10 6
done
Uptime: 2m45s
ata0: resetting devices.. done
Rebooting...
```

- Related Documentation**
- [Checking the Status of a Device Running Junos OS on page 436](#)
 - [Displaying Junos OS Information on page 577](#)

Using the Junos OS CLI Comment Character # for Operational Mode Commands

The comment character in Junos OS enables you to copy operational mode commands that include comments from a file and paste them into the CLI. A pound sign (#) at the beginning of the command-line indicates a comment line. This is useful for describing frequently used operational mode commands; for example, a user's work instructions on how to monitor the network. To add a comment to a command file, the first character of the line must be #. When you start a command with #, the rest of the line is disregarded by Junos OS.

To add comments in operational mode, start with a # and end with a new line (carriage return):

```
user@host> # comment-string
```

comment-string is the text of the comment. The comment text can be any length, but each comment line must begin with a #.

- Related Documentation**
- [Example: Using Comments in Junos OS Operational Mode Commands on page 584](#)

Example: Using Comments in Junos OS Operational Mode Commands

The following example shows how to use comments in a file:

```
#Command 1: Show the router version
show version
#Command 2: Show all router interfaces
show interfaces terse
```

The following example shows how to copy and paste contents of a file into the CLI:

```
user@host> #Command 1: Show the router version
user@host> show version
Hostname: myhost
Model: m5
```



```

Junos Base OS boot [6.4-20040511.0]
Junos Base OS Software Suite [6.4-20040511.0]
Junos Kernel Software Suite [6.4-20040511.0]
Junos Packet Forwarding Engine Support (M5/M10) [6.4-20040511.0] Junos Routing
  Software Suite [6.4-20040511.0] Junos Online Documentation [6.4-20040511.0] Junos
  Crypto Software Suite [6.4-20040511.0]
user@host> # Command 2: Show all router interfaces
user@host> show interfaces terse
Interface Admin Link Proto Local Remote
fe-0/0/0 up up
fe-0/0/1 up down
fe-0/0/2 up down
mo-0/1/0 up
mo-0/1/0.16383 up up inet 10.0.0.1 --> 10.0.0.17
so-0/2/0 up up
so-0/2/1 up up
dsc up up
fxp0 up up
fxp0.0 up up inet 192.168.70.62/21
fxp1 up up
fxp1.0 up up tnp 4
gre up up
ipip up up
lo0 up up
lo0.0 up up inet 127.0.0.1 --> 0/0
lo0.16385 up up inet

```

- Related Documentation**
- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 584](#)

Filtering Command Output

- [Using the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 587](#)
- [Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 588](#)
- [Filtering Operational Mode Command Output in a QFabric System on page 589](#)
- [Pipe \(| \) Filter Functions in the Junos OS Command-Line Interface on page 590](#)

Using the Pipe (|) Symbol to Filter Junos OS Command Output

The Junos OS enables you to filter command output by adding the pipe (|) symbol when you enter a command.

For example:

```
user@host> show rip neighbor ?
Possible completions:
<[Enter]>      Execute this command
<name>         Name of RIP neighbor
instance       Name of RIP instance
logical-system Name of logical system, or 'all'
|              Pipe through a command
```

The following example lists the filters that can be used with the pipe symbol (|):

```
user@host> show interfaces | ?
user@host> show interfaces | ?
Possible completions:
append      Append output text to file
count       Count occurrences
display     Show additional kinds of information
except      Show only text that does not match a pattern
find        Search for first occurrence of pattern
hold        Hold text without exiting the --More-- prompt
last        Display end of output only
match       Show only text that matches a pattern
no-more     Don't paginate output
refresh     Refresh a continuous display of the command
request     Make system-level requests
resolve     Resolve IP addresses
save        Save output text to file
tee         Write to standard output and file
trim        Trim specified number of columns from start of line
```

For the **show configuration** command only, an additional compare filter is available:

```
user@host> show configuration | ?
Possible completions:
  compare          Compare configuration changes with prior version
  ...
```

You can enter any of the pipe filters in conjunction. For example:

```
user@host> command | match regular-expression | save filename
```



NOTE: This topic describes *only* the filters that can be used for operational mode command output. For information about filters that can be used in configuration mode, see the *Junos OS Administration Library for Routing Devices*.

Related Documentation

- [Pipe \(| \) Filter Functions in the Junos OS Command-Line Interface on page 590](#)
- [Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 588](#)
- [Filtering Operational Mode Command Output in a QFabric System on page 589](#)

Using Regular Expressions with the Pipe (|) Symbol to Filter Junos OS Command Output

The **except**, **find**, and **match** filters used with the pipe symbol employ regular expressions to filter output. Juniper Networks uses the regular expressions as defined in POSIX 1003.2. If the regular expressions contain spaces, operators, or wildcard characters, enclose the expression in quotation marks.

Table 64: Common Regular Expression Operators in Operational Mode Commands

Operator	Function
	Indicates that a match can be one of the two terms on either side of the pipe.
^	Used at the beginning of an expression, denotes where a match should begin.
\$	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the \$ character.
[]	Specifies a range of letters or digits to match. To separate the start and end of a range, use a hyphen (-).
()	Specifies a group of terms to match.

For example, if a command produces the following output:

```

12
22
321
4

```

a pipe filter of **| match 2** displays the following output:

```

12
22
321

```

and a pipe filter of **| except 1** displays the following output:

```

22
4

```

Related Documentation

- [Using the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 587](#)
- [Pipe \(| \) Filter Functions in the Junos OS Command-Line Interface on page 590](#)

Filtering Operational Mode Command Output in a QFabric System

When you issue an operational mode command in a QFabric system, the output generated can be fairly extensive because of the number of components contained within the system. To make the output more accessible, you can filter the output by appending the **| filter** option to the end of most Junos OS commands.

1. To filter operational mode command output and limit it to a Node group, include the **| filter node-group *node-group-name*** option at the end of your Junos OS operational mode command.

```
root@qfabric> show interfaces terse | filter node-group NW-NG-0
```

Interface	Admin	Link	Proto	Local	Remote
NW-NG-0:dsc	up	up			
NW-NG-0:em0	up	up			
NW-NG-0:em1	up	up			
NW-NG-0:gre	up	up			
NW-NG-0:ipip	up	up			
NW-NG-0:lo0	up	up			
NW-NG-0:lo0.16384	up	up	inet	127.0.0.1	--> 0/0
NW-NG-0:lo0.16385	up	up	inet		
NW-NG-0:lsi	up	up			
NW-NG-0:mtun	up	up			
NW-NG-0:pimd	up	up			
NW-NG-0:pime	up	up			
NW-NG-0:tap	up	up			
Node01:ge-0/0/10	up	up			
Node01:ge-0/0/40	up	up			
Node01:ge-0/0/41	up	up			
vlan	up	up			

2. To filter operational mode command output and limit it to a set of Node groups, include the **| filter node-group** option at the end of your Junos OS operational mode command and specify the list of Node group names in brackets.

```
root@qfabric> show ethernet-switching interfaces | filter node-group [NW-NG-0 RSNG-1]
```

Interface	State	VLAN members	Tag	Tagging	Blocking
NW-NG-0:ae0.0	up	v200	200	tagged	unblocked
		v50	50	tagged	unblocked
		v51	51	tagged	unblocked
		v52	52	tagged	unblocked
		v53	53	tagged	unblocked
RSNG-1:ae0.0	up	v200	200	untagged	unblocked
RSNG-1:ae47.0	up	v50	50	tagged	unblocked
		v51	51	tagged	unblocked
		v52	52	tagged	unblocked
		v53	53	tagged	unblocked

- Related Documentation**
- [QFabric System Operational Mode Commands](#)
 - [Using the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 587](#)

Pipe (|) Filter Functions in the Junos OS Command-Line Interface

This topic describes the pipe (|) filter functions that are supported in the Junos OS command-line interface (CLI):

- [Comparing Configurations and Displaying the Differences in Text on page 590](#)
- [Comparing Configurations and Displaying the Differences in XML on page 592](#)
- [Counting the Number of Lines of Output on page 592](#)
- [Displaying Output in XML Tag Format on page 592](#)
- [Displaying Output in JSON Format on page 593](#)
- [Displaying the RPC tags for a Command on page 593](#)
- [Ignoring Output That Does Not Match a Regular Expression on page 593](#)
- [Displaying Output from the First Match of a Regular Expression on page 594](#)
- [Retaining Output After the Last Screen on page 594](#)
- [Displaying Output Beginning with the Last Entries on page 594](#)
- [Displaying Output That Matches a Regular Expression on page 595](#)
- [Preventing Output from Being Paginated on page 595](#)
- [Sending Command Output to Other Users on page 595](#)
- [Resolving IP Addresses on page 596](#)
- [Saving Output to a File on page 596](#)
- [Appending Output to a File on page 596](#)
- [Displaying Output on Screen and Writing to a File on page 597](#)
- [Trimming Output by Specifying the Starting Column on page 597](#)
- [Refreshing the Output of a Command on page 597](#)

Comparing Configurations and Displaying the Differences in Text

The **compare** filter compares the candidate configuration with either the current committed configuration or a configuration file and displays the differences between

the two configurations with text characters. To compare configurations, enter **compare** after the pipe (|) symbol:

```
[edit]
user@host# show | compare [filename] rollback n]
```

filename is the full path to a configuration file.

n is the index into the list of previously committed configurations. The most recently saved configuration is 0. If you do not specify arguments, the candidate configuration is compared against the active configuration file (**/config/juniper.conf**).

The comparison output uses the following conventions:

- Statements that are only in the candidate configuration are prefixed with a plus sign (+).
- Statements that are only in the comparison file are prefixed with a minus sign (-).
- Statements that are unchanged are prefixed with a single blank space ().

For example:

```
user@host> show configuration system | compare rollback 9
[edit system]
+ host-name device;
+ backup-router 192.168.71.254;
- ports {
-     console log-out-on-disconnect;
- }
[edit system name-server]
+ 172.17.28.11;
  172.17.28.101 { ... }
[edit system name-server]
  172.17.28.101 { ... }
+ 172.17.28.100;
+ 172.17.28.10;
[edit system]
- scripts {
-     commit {
-         allow-transients;
-     }
- }
+ services {
+     ftp;
+     rlogin;
+     rsh;
+     telnet;
+ }
```

Starting with Junos OS Release 8.3, output from the **show | compare** command has been enhanced to more accurately reflect configuration changes. This includes more intelligent handling of order changes in lists. For example, consider names in a group that are reordered as follows:

```
groups {      groups {
group_xmp;    group_xmp;
group_cmp;    group_grp:
group_grp;    group_cmp;
}             }
```

In previous releases, output from the **show | compare** command looked like the following:

```
[edit groups]
- group_xmp;
- group_cmp;
- group_grp;
+ group_xmp;
+ group_grp;
+ group_cmp;
```

Now, output from the **show | compare** command looks like the following:

```
[edit groups]
group_xmp {...}
! group_grp {...}
```

Comparing Configurations and Displaying the Differences in XML

The **compare | display xml** filter compares the candidate configuration with the current committed configuration and displays the differences between the two configurations in XML. To compare configurations, enter **compare | display xml** after the pipe (|) symbol in either operational or configuration mode.

Example in operational mode:

```
user@host> show configuration | compare | display xml
```

Example in configuration mode:

```
[edit]
user@host# show | compare | display xml
```

You can enter a specific configuration hierarchy prior to **| compare**. In configuration mode, you can navigate to a hierarchy where the command is applied.

For a description of the XML output, see [“Understanding the show | compare | display xml Command Output” on page 528](#).

Counting the Number of Lines of Output

To count the number of lines in the output from a command, enter **count** after the pipe symbol (|). For example:

```
user@host> show configuration | count
Count: 269 lines
```

Displaying Output in XML Tag Format

To display command output in XML tag format, enter **display xml** after the pipe symbol (|).

The following example displays the **show cli directory** command output as XML tags:

```
user@host> show cli directory | display xml
<rpc-reply xmlns:junos="http://xml.juniper.net/junos/7.5I0/junos">
  <cli>
    <working-directory>/var/home/user</working-directory>
  </cli>
```



```

    <cli>
      <banner></banner>
    </cli>
  </rpc-reply>

```

To display the change in the candidate and active configurations in XML tag format, see [“Comparing Configurations and Displaying the Differences in XML” on page 592](#)

Displaying Output in JSON Format

To display command output in JavaScript Object Notation (JSON) format, enter **display json** after the pipe symbol (|).

The following example displays the **show cli directory** command output in JSON format:

```
user@host> show cli directory | display json
```

```

{
  "cli" : [
    {
      "working-directory" : [
        {
          "data" : "/var/home/username"
        }
      ]
    }
  ]
}

```

Displaying the RPC tags for a Command

To display the remote procedure call (RPC) XML tags for an operational mode command, enter **display xml rpc** after the pipe symbol (|).

The following example displays the RPC tags for the **show route** command:

```

user@host> show route | display xml rpc
<rpc-reply xmlns:junos="http://xml.juniper.net/junos/10.1I0/junos">
  <rpc>
    <get-route-information>
    </get-route-information>
  </rpc>
  <cli>
    <banner></banner>
  </cli>
</rpc-reply>

```

Ignoring Output That Does Not Match a Regular Expression

To ignore text that matches a regular expression, specify the **except** command after the pipe symbol (|). If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. For information on common regular expression operators, see [“Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output” on page 588](#).

The following example displays all users who are logged in to the router, except for the user **root**:

```
user@host> show system users | except root
 8:28PM up 1 day, 13:59, 2 users, load averages: 0.01, 0.01, 0.00
USER   TTY FROM                LOGIN@  IDLE WHAT
user   p0  device1.example.com  7:25PM    - cli
```

Displaying Output from the First Match of a Regular Expression

To display output starting with the first occurrence of text matching a regular expression, enter **find** after the pipe symbol (|). If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. For information on common regular expression operators, see [“Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output” on page 588](#).

The following example displays the routes in the routing table starting at IP address **208.197.169.0**:

```
user@host> show route | find 208.197.169.0
208.197.169.0/24    *[Static/5] 1d 13:22:11
                  > to 192.168.4.254 via so-3/0/0.0
224.0.0.5/32      *[OSPF/10] 1d 13:22:12, metric 1
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
47.0005.80ff.f800.0000.0108.0001.1921.6800.4015.00/160
                  *[Direct/0] 1d 13:22:12
                  > via lo0.0
```

The following example displays the first CCC entry in the forwarding table:

```
user@host> show route forwarding-table | find ccc
Routing table: ccc
MPLS:
Interface.Label   Type RtRef Nexthop          Type Index NhRef Netif
default           perm  0          10.0.16.2                rjct   3    1
0                 user  0          10.0.16.2                recv   5    2
1                 user  0          10.0.16.2                recv   5    2
32769             user  0          10.0.16.2                ucst   45   1 fe-0/0/0.534
fe-0/0/0. (CCC)   user  0          10.0.16.2                indr   44   2
                                     Push 32768, Push
```

Retaining Output After the Last Screen

To not return immediately to the CLI prompt after viewing the last screen of output, enter **hold** after the pipe symbol (|). The following example prevents returning to the CLI prompt after you have viewed the last screen of output from the **show log log-file-1** command:

```
user@host> show log log-file-1 | hold
```

This filter is useful when you want to scroll or search through output.

Displaying Output Beginning with the Last Entries

To display text starting from the end of the output, enter **last <lines>** after the pipe symbol (|).

The following example displays the last entries in **log-file-1** file:

```
user@host> show log log-file-1 | last
```

This filter is useful for viewing log files in which the end of the file contains the most recent entries.



NOTE: When the number of lines requested is less than the number of lines that the screen length setting permits you to display, Junos returns as many lines as permitted by the screen length setting. That is, if your screen length is set to 20 lines and you have requested only the last 10 lines, Junos returns the last 19 lines instead of the last 10 lines.

Displaying Output That Matches a Regular Expression

To display output that matches a regular expression, enter **match *regular-expression*** after the pipe symbol (|). If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. For information on common regular expression operators, see [“Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output” on page 588](#).

The following example matches all the Asynchronous Transfer Mode (ATM) interfaces in the configuration:

```
user@host> show configuration | match at-
at-2/1/0 {
at-2/1/1 {
at-2/2/0 {
at-5/2/0 {
at-5/3/0 {
```

Preventing Output from Being Paginated

By default, if output is longer than the length of the terminal screen, you are provided with a **---(more)---** message to display the remaining output. To display the remaining output, press the Spacebar.

To prevent the output from being paginated, enter **no-more** after the pipe symbol (|).

The following example displays output from the **show configuration** command all at once:

```
user@host> show configuration | no-more
```

This feature is useful, for example, if you want to copy the entire output and paste it into an e-mail.

Sending Command Output to Other Users

To display command output on the terminal of a specific user logged in to your router, or on the terminals of all users logged in to your router, enter **request message (all | user *account@terminal*)** after the pipe symbol (|).

If you are troubleshooting your router and, for example, talking with a customer service representative on the phone, you can use the **request message** command to send your representative the command output you are currently viewing on your terminal.

The following example sends the output from the **show interfaces** command you enter on your terminal to the terminal of the user **root@tty1**:

```
user@host> show interfaces | request message user root@tty1
```

The user **root@tty1** sees the following output appear on the terminal screen:

```
Message from user@host on /dev/tty0 at 10:32 PST...
Physical interface: dsc, Enabled, Physical link is Up
  Interface index: 5, SNMP ifIndex: 5
  Type: Software-Pseudo, MTU: Unlimited...
```

Resolving IP Addresses

In operational mode only, if the output of a command displays an unresolved IP address, you can enter **| resolve** after the command to display the name associated with the IP address. The **resolve** filter enables the system to perform a reverse DNS lookup of the IP address. If DNS is not enabled, the lookup fails and no substitution is performed.

To perform a reverse DNS lookup of an unresolved IP address, enter **resolve <full-names>** after the pipe symbol (**|**). If you do not specify the **full-names** option, the name is truncated to fit whatever field width limitations apply to the IP address.

The following example performs a DNS lookup on any unresolved IP addresses in the output from the **show ospf neighbors** command:

```
user@host> show ospf neighbors | resolve
```

Saving Output to a File

When command output is lengthy, when you need to store or analyze the output, or when you need to send the output in an e-mail or by FTP, you can save the output to a file. By default, the file is placed in your home directory on the router.

To save command output to a file, enter **save filename** after the pipe symbol (**|**).

The following example saves the output from the **request support information** command to a file named **my-support-info.txt**:

```
user@host> request support information | save my-support-info.txt
Wrote 1143 lines of output to 'my-support-info.txt'
user@host>
```

Appending Output to a File

When command output is displayed, you can either save the output to a file, which overwrites the existing contents of that file or you can append the output text to a specific file.

To append the command output to the file, enter **append filename** after the pipe symbol (**|**).

The following example appends the output from the **request support information** command to a file named **my-support-info.txt**:

```
user@host> request support information | append my-support-info.txt
Wrote 2247 lines of output to 'my-support-info.txt'
user@host>
```

Displaying Output on Screen and Writing to a File

When command output is displayed, you can also write the output to a file. To both display the output and write it to a file, enter **tee filename** after the pipe symbol (**|**).

The following example displays the output from the **show interfaces ge-* terse** command (displaying information about the status of the gigabit Ethernet interfaces on the device) and diverts the output to a file called **ge-interfaces.txt**:

```
user@host> show interfaces ge-* terse | tee ge-interfaces.txt
Interface           Admin Link Proto  Local           Remote
ge-0/1/0             up    down
ge-0/1/1             up    up
ge-0/1/2             up    down
ge-0/1/3             up    up
```

Unlike the UNIX **tee** command, only an error message is displayed if the file cannot be opened (instead of displaying the output and then the error message).

```
user@host> show interfaces ge-* terse | tee /home/user/test.txt
error: tee failed: file /home/user/test.txt could not be opened

user@host>
```

Trimming Output by Specifying the Starting Column

Output appears on the terminal screen in terms of rows and columns. The first alphanumeric character starting at the left of the screen is in column 1, the second character is in column 2, and so on. To display output starting from a specific column (thus trimming the leftmost portion of the output), enter **trim columns** after the pipe symbol (**|**). The **trim** filter is useful for trimming the date and time from the beginning of system log messages.

The following example displays output from the **show system storage** command, filtering out the first 10 columns:

```
user@host> show system storage | trim 11
```



NOTE: The **trim** command does not accept negative values.

Refreshing the Output of a Command

You can run an operational mode command with the **| refresh** pipe option to refresh the output displayed on the screen periodically. The default refresh occurs every second. However, you can also explicitly specify a refresh interval from 1 through 604800 seconds.

For example, to refresh the output of the **show interfaces** command every five seconds, you would run the following command:

```
user@host > show interfaces | refresh 5
```

**Related
Documentation**

- [Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 588](#)
- [Using the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 587](#)

CHAPTER 27

Using Shortcuts, Wildcards, and Regular Expressions in the CLI

- Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 599
- Using Wildcard Characters in Interface Names on page 601
- Common Regular Expressions to Use with the replace Command on page 602
- Using Global Replace in the Junos OS Configuration on page 603
- Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference on page 604
- Example: Using Global Replace in a Junos OS Configuration—Replacing an Interface Name on page 606
- Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608
- Using Regular Expressions to Delete Related Items from a Junos OS cConfiguration on page 609

Using Keyboard Sequences to Move Around and Edit the Junos OS CLI

You can use keyboard sequences in the Junos OS command-line interface (CLI) to move around and edit the command line. You can also use keyboard sequences to scroll through a list of recently executed commands. [Table 65](#) lists some of the CLI keyboard sequences. They are the same as those used in Emacs.

Table 65: CLI Keyboard Sequences

Category	Action	Keyboard Sequence
Move the Cursor	Move the cursor back one character.	Ctrl+b
	Move the cursor back one word.	Esc+b or Alt+b
	Move the cursor forward one character.	Ctrl+f
	Move the cursor forward one word.	Esc+f or Alt+f
	Move the cursor to the beginning of the command line.	Ctrl+a
	Move the cursor to the end of the command line.	Ctrl+e
Delete Characters	Delete the character before the cursor.	Ctrl+h, Delete, or Backspace
	Delete the character at the cursor.	Ctrl+d
	Delete all characters from the cursor to the end of the command line.	Ctrl+k
	Delete all characters on the command line.	Ctrl+u or Ctrl+x
	Delete the word before the cursor.	Ctrl+w, Esc+Backspace, or Alt+Backspace
	Delete the word after the cursor.	Esc+d or Alt+d
Insert Recently Deleted Text	Insert the most recently deleted text at the cursor.	Ctrl+y
Redraw the Screen	Redraw the current line.	Ctrl+l

Table 65: CLI Keyboard Sequences (*continued*)

Category	Action	Keyboard Sequence
Display Previous Command Lines	Scroll backward through the list of recently executed commands.	Ctrl+p
	Scroll forward through the list of recently executed commands.	Ctrl+n
	Search the CLI history in reverse order for lines matching the search string.	Ctrl+r
	Search the CLI history by typing some text at the prompt, followed by the keyboard sequence. The CLI attempts to expand the text into the most recent word in the history for which the text is a prefix.	Esc+/ sequence
Display Previous Command Words	Scroll backward through the list of recently entered words in a command line.	Esc+. or Alt+.
Repeat Keyboard Sequences	Specify the number of times to execute a keyboard sequence. <i>number</i> can be from 1 through 9 and <i>sequence</i> is the keyboard sequence that you want to execute.	Esc+ <i>number</i> sequence or Alt+ <i>number</i> sequence

- Related Documentation**
- [Using Wildcard Characters in Interface Names on page 601](#)
 - [Using Global Replace in a Junos OS Configuration on page 603](#)

Using Wildcard Characters in Interface Names

You can use wildcard characters in the Junos OS operational commands to specify groups of interface names without having to type each name individually. [Table 66](#) lists the available wildcard characters. You must enclose all wildcard characters except the asterisk (*) in quotation marks (" ").

Table 66: Wildcard Characters for Specifying Interface Names

Wildcard Character	Description
* (asterisk)	Match any string of characters in that position in the interface name. For example, so* matches all SONET/SDH interfaces.
"[<i>character</i> < <i>character</i> ...>]"	Match one or more individual characters in that position in the interface name. For example, so-"[03]"* matches all SONET/SDH interfaces in slots 0 and 3.

Table 66: Wildcard Characters for Specifying Interface Names (*continued*)

Wildcard Character	Description
"[!character<character...>]"	Match all characters except the ones included in the brackets. For example, so- "[!03]" * matches all SONET/SDH interfaces except those in slots 0 and 3.
"[character1-character2]"	Match a range of characters. For example, so- "[0-3]" * matches all SONET/SDH interfaces in slots 0, 1, 2, and 3.
"[!character1-character2]"	Match all characters that are not in the specified range of characters. For example, so- "[!0-3]" * matches all SONET/SDH interfaces in slots 4, 5, 6, and 7.

- Related Documentation**
- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 599](#)
 - [Using Global Replace in a Junos OS Configuration on page 603](#)

Common Regular Expressions to Use with the replace Command

Table 67: Common Regular Expressions to Use with the replace Command

Operator	Function
	Indicates that a match can be one of the two terms on either side of the pipe.
^	Used at the beginning of an expression, denotes where a match should begin.
\$	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the \$ character.
[]	Specifies a range of letters or digits to match. To separate the start and end of a range, use a hyphen (-).
()	Specifies a group of terms to match. Stored as numbered variables. Use for back references as \1 \2 \9.
*	0 or more terms.
+	One or more terms.
.	Any character except for a space (" ").
\	A backslash escapes special characters to suppress their special meaning. For example, \. matches . (period symbol).
\n	Back reference. Matches the <i>n</i> th group.
&	Back reference. Matches the entire match.

Table 68 lists some replacement examples.

Table 68: Replacement Examples

Command	Result
<code>replace pattern myrouter with router1</code>	Match: <code>myrouter</code> Result: <code>router1</code>
<code>replace pattern "192.168\.(.*)/24" with "10.2.1/28"</code>	Match: <code>192.168.3.4/24</code> Result: <code>10.2.3.4/28</code>
<code>replace pattern "1.1" with "abc&def"</code>	Match: <code>1.1</code> Result: <code>abc1.1def</code>
<code>replace pattern 1.1 with "abc\&def"</code>	Match: <code>1#1</code> Result: <code>abc&def</code>

Related Documentation

- [Using Global Replace in a Junos OS Configuration on page 603](#)
- [Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference on page 604](#)

Using Global Replace in the Junos OS Configuration

You can make global changes to variables and identifiers in the Junos OS configuration by using the **replace** configuration mode command. This command replaces a pattern in a configuration with another pattern. For example, you can use this command to find and replace all occurrences of an interface name when a PIC is moved to another slot in the router.

```
user@host# replace pattern pattern1 with pattern2 <upto n>
```

pattern *pattern1* is a text string or regular expression that defines the identifiers and values you want to replace in the configuration.

pattern2 is a text string or regular expression that replaces the identifiers and values located with *pattern1*.

Juniper Networks uses standard UNIX-style regular expression syntax (as defined in POSIX 1003.2). If the regular expression contains spaces, operators, or wildcard characters, enclose the expression in quotation marks. Greedy qualifiers (match as much as possible) are supported. Lazy qualifiers (match as little as possible) are not.

The **upto *n*** option specifies the number of objects replaced. The value of *n* controls the total number of objects that are replaced in the configuration (not the total number of times the pattern occurs). Objects at the same hierarchy level (siblings) are replaced first. Multiple occurrences of a pattern within a given object are considered a single replacement. For example, if a configuration contains a **010101** text string, the command

replace pattern 01 with pattern 02 upto 2 replaces 010101 with 020202 (instead of 020201). Replacement of 010101 with 020202 is considered a single replacement ($n = 1$), not three separate replacements ($n = 3$).

If you do not specify an **upto** option, all identifiers and values in the configuration that match *pattern1* are replaced.

The **replace** command is available in configuration mode at any hierarchy level. All matches are case-sensitive.

Related Documentation

- [Common Regular Expressions to Use with the replace Command on page 602](#)
- [Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference on page 604](#)
- [Example: Using Global Replace in a Junos OS Configuration—Replacing an Interface Name on page 606](#)
- [Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608](#)
- [Using Wildcard Characters in Interface Names on page 601](#)
- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 599](#)

Example: Using Global Replace in a Junos OS Configuration—Using the \n Back Reference

This example shows how you can use a backreference to replace a pattern.

- [Requirements on page 604](#)
- [Overview on page 605](#)
- [Configuration on page 605](#)

Requirements

No special configuration beyond device initiation is required before configuring this example.

Before you begin, configure the following:

```
[edit]
user@host# show interfaces
xe-0/0/0 {
    unit 0;
}
fe-3/0/1 {
    vlan-tagging;
    unit 0 {
        description "inet6 configuration. IP: 2000::c0a8::1bf5";
        vlan-id 100;
        family inet {
            address 17.10.1.1/24;
        }
    }
}
```

```

    family inet6 {
        address 2000::c0a8:1bf5/3;
    }
}

```

To quickly configure this initial configuration, copy the following commands and paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

```

set interfaces xe-0/0/0 unit 0
set interfaces fe-3/0/1 vlan-tagging
set interfaces fe-3/0/1 unit 0 description "inet6 configuration IP: 2000::c0a8:1bf5"
set interfaces fe-3/0/1 unit 0 vlan-id 100
set interfaces fe-3/0/1 unit 0 family inet address 17.10.1.1/24
set interfaces fe-3/0/1 unit 0 family inet6 address 2000::c0a8:1bf5/3

```

Overview

One of the most useful features of regular expressions is the backreference. Backreferences provide a convenient way to identify a repeated character or substring within a string. Once you find the pattern, you can repeat it without writing it again. You refer to the previously captured pattern with just `\#` (where `#` is a numeral that indicates the number of times you want the pattern matched).

You can use backreferences to recall, or find, data and replace it with something else. In this way you can reformat large sets of data with a single replace command, thus saving you the time it would take to look for and replace the pattern manually.

Configuration

Configuring a Replacement Using a Backreference in the Command

Step-by-Step Procedure

To replace a pattern in a Junos OS configuration using a backreference:

- Use the **replace** command.

```

[edit]
user@host# replace pattern pattern1 with pattern2

```

In this case, we want to replace `:.1bf5` with `1bf5`.

```

[edit]
user@host# replace pattern "(.*)1bf5" with "\11bf5"

```

Notice the backreference (`\1`), which indicates the pattern should be searched for and replaced only once.

Results

Here is the resulting configuration:

```

[edit]
user@host# show interfaces
xe-0/0/0 {

```

```

    unit 0;
  }
  fe-3/0/1 {
    vlan-tagging;
    unit 0 {
      description "inet6 configuration. IP: 2000::c0a8:1bf5";
      vlan-id 100;
      family inet {
        address 17.10.1.1/24;
      }
      family inet6 {
        address 2000::c0a8:1bf5/3;
      }
    }
  }
}

```

In this example, the pattern 2000::c0a8:1bf5 is replaced with 2000::c0a8:1bf5 once.

- Related Documentation**
- [Example: Using Global Replace in a Junos OS Configuration—Replacing an Interface Name on page 606](#)
 - [Using Global Replace in a Junos OS Configuration on page 603](#)

Example: Using Global Replace in a Junos OS Configuration—Replacing an Interface Name

This example shows how to replace an interface name globally in a configuration by using the **replace** command.

Using the **replace** command can be a faster and better way to change a configuration. For example, a PIC might be moved to another slot in a router, which changes the interface name. With one command you can update the whole configuration. Or you might want to quickly extend the configuration with other similar configurations, for example, similar interfaces. By using a combination of the **copy** and **replace** commands, you can add to a configuration and then replace certain aspects of the newly copied configurations. The **replace** command works with regular expressions. Regular expressions are quick, flexible, and ubiquitous. You can fashion just about any pattern you might need to search for, and most programming languages support regular expressions.

- [Requirements on page 606](#)
- [Overview on page 607](#)
- [Configuration on page 607](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Before you begin, configure the following hierarchy on the router. To quickly configure this hierarchy, see “[CLI Quick Configuration](#)” on page 495 .

```
user@host# show interfaces
```

```

so-0/0/0 {
  dce;
}
user@host# show protocols
ospf {
  area 0.0.0.0 {
    interface so-0/0/0.0 {
      hello-interval 5;
    }
  }
}

```

Overview

This example shows how to replace an interface name globally in a configuration by using the **replace** command. It is a simple example.

The previous configuration is the starting point for this configuration update. In the course of this example, you change the name of the initial interface throughout the configuration with one command.

Configuration

CLI Quick Configuration To quickly configure the initial configuration for this example, copy the following commands, paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste these commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.:

```

set interfaces so-0/0/0 dce
set protocols ospf area 0.0.0.0 interface so-0/0/0.0 hello-interval 5

```

Configuring an Interface Name Change

Step-by-Step Procedure To change an interface name:

1. Make sure that you are at the top of the configuration mode hierarchy.

```
user@host# top
```
2. Replace so-0/0/0 with so-1/1/0 using the **replace** command, which uses the **pattern** keyword.

```
user@host# replace pattern so-0/0/0 with so-1/1/0
```

Results

After making the required changes, verify the configuration by using the **show interfaces** and **show protocols** configuration mode commands.

```

[edit]
user@host# show interfaces
so-1/1/0 {
  dce;
}
user@host# show protocols

```

```
ospf {
  area 0.0.0.0 {
    interface so-1/1/0.0 {
      hello-interval 5;
    }
  }
}
```

After you have confirmed that the configuration is correct, enter the **commit** command.

Related Documentation

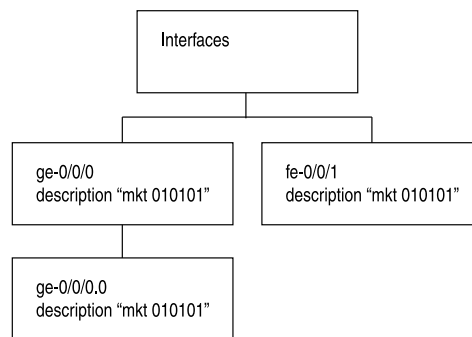
- [Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608](#)
- [Using Global Replace in a Junos OS Configuration on page 603](#)
- [Examples: Re-Using Configuration on page 476](#)

Example: Using Global Replace in a Junos OS Configuration—Using the upto Option

Consider the hierarchy shown in [Figure 23](#). The text string **010101** appears in three places: the description sections of **ge-0/0/0**, **ge-0/0/0.0**, and **fe-0/0/1**. These three instances are three objects. The following example shows how you can use the **upto** option to perform replacements in a JUNOS configuration:

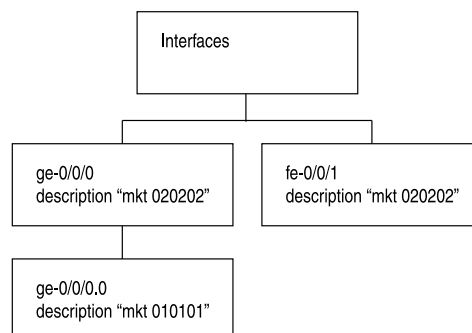
Figure 23: Replacement by Object

Current Configuration:



user@host > **replace pattern 01 with pattern 02 upto 2**

Resulting Configuration:



g017228

An **upto 2** option in the **replace** command converts **01** to **02** for two object instances. The objects under the main interfaces **ge-0/0/0** and **fe-0/0/1** will be replaced first (since these are siblings in the hierarchy level). Because of the **upto 2** restriction, the **replace** command replaces patterns in the first and second instance in the hierarchy (siblings), but not the third instance (child of the first instance).

```

user@host# show interfaces
ge-0/0/0 {
  description "mkt 010101"; #First instance in the hierarchy
  unit 0 {
    description "mkt 010101"; #Third instance in the hierarchy (child of the first
    instance)
  }
}
fe-0/0/1 {
  description "mkt 010101"; #second instance in the hierarchy (sibling of the first
  instance)
  unit 0 {
    family inet {
      address 200.200.20.2/24;
    }
  }
}
[edit]
user@host# replace pattern 01 with 02 upto 2
[edit]
user@host# commit
commit complete

[edit]
user@host# show interfaces
ge-0/0/0 {
  description "mkt 020202"; #First instance in the hierarchy
  unit 0 {
    description "mkt 010101"; #Third instance in the hierarchy (child of the first
    instance)
  }
}
fe-0/0/1 {
  description "mkt 020202"; #second instance in the hierarchy (sibling of the first
  instance)
  unit 0 {
    family inet {
      address 200.200.20.2/24;
    }
  }
}

```

Related Documentation • [Using Global Replace in a Junos OS Configuration on page 603](#)

Using Regular Expressions to Delete Related Items from a Junos OS cConfiguration

The Junos OS command-line interface (CLI) enables you to delete related configuration items simultaneously, such as channelized interfaces or static routes, by using a single

command and regular expressions. Deleting a statement or an identifier effectively “unconfigures” the functionality associated with that statement or identifier, returning that functionality to its default condition.

You can only delete certain parts of the configuration where you normally put multiple items, for example, interfaces. However, you cannot delete “groups” of different items; for example:

```
user@host# show system services
ftp;
rlogin;
rsh;
ssh {
    root-login allow;
}
telnet;
[edit]
user@host# wildcard delete system services *
syntax error.
```

When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration.

To delete related configuration items, issue the **wildcard** configuration mode command with the **delete** option and specify the statement path, the items to be summarized with a regular expression, and the regular expression.

```
user@host# wildcard delete <statement-path> <identifier> <regular-expression>
```



NOTE: When you use the **wildcard** command to delete related configuration items, the regular expression must be the final statement.

If the Junos OS matches more than eight related items, the CLI displays only the first eight items.

Deleting Interfaces from the Configuration

Delete multiple T1 interfaces in the range from t1-0/0/0:0 through t1-0/0/0:23:

```
user@host# wildcard delete interfaces t1-0/0/0:.*
matched: t1-0/0/0:0
matched: t1-0/0/0:1
matched: t1-0/0/0:2
Delete 3 objects? [yes,no] (no) no
```

**Deleting Routes from
the Configuration**

Delete static routes in the range from 172.0.0.0 to 172.255.0.0:

```
user@host# wildcard delete routing-options static route 172.*
matched: 172.16.0.0/12
matched: 172.16.14.0/24
matched: 172.16.100.0/24
matched: 172.16.128.0/19
matched: 172.16.160.0/24
matched: 172.17.12.0/23
matched: 172.17.24.0/23
matched: 172.17.28.0/23
...
Delete 13 objects? [yes,no] (no)
```

**Related
Documentation**

- [Disabling Inheritance of a Junos OS Configuration Group on page 620](#)

CHAPTER 28

Using Configuration Groups to Quickly Configure Devices

- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating the Junos OS Configuration Group on page 615](#)
- [Applying the Junos OS Configuration Group on page 617](#)
- [Example: Configuring and Applying Junos OS Configuration Groups on page 618](#)
- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 619](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 620](#)
- [Using Wildcards with Configuration Groups on page 622](#)
- [Example: Configuring Sets of Statements with Configuration Groups on page 625](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 626](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 628](#)
- [Example: Configuring Peer Entities on page 630](#)
- [Establishing Regional Configurations on page 631](#)
- [Configuring Wildcard Configuration Group Names on page 633](#)
- [Example: Referencing the Preset Statement From the Junos OS defaults Group on page 634](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 635](#)
- [Using Conditions to Apply Configuration Groups Overview on page 636](#)
- [Example: Configuring Conditions for Applying Configuration Groups on page 636](#)
- [Improving Commit Time When Using Configuration Groups on page 638](#)
- [Example: Improving Commit Time When Using Configuration Groups on page 639](#)
- [Using Junos OS Defaults Groups on page 640](#)
- [Set Up Routing Engine Configuration Groups on page 642](#)

Understanding Junos OS Configuration Groups

This topic provides an overview of the configuration groups feature and the inheritance model in Junos OS, and contains the following sections:

- [Configuration Groups Overview on page 614](#)
- [Inheritance Model on page 614](#)
- [Configuring Configuration Groups on page 614](#)

Configuration Groups Overview

The configuration groups feature in Junos OS enables you to create a group containing configuration statements and to direct the inheritance of that group's statements in the rest of the configuration. The same group can be applied to different sections of the configuration, and different sections of one group's configuration statements can be inherited in different places in the configuration.

Configuration groups enable you to create smaller, more logically constructed configuration files, making it easier to configure and maintain Junos OS. For example, you can group statements that are repeated in many places in the configuration, such as when configuring interfaces, and thereby limit updates to just the group.

You can also use wildcards in a configuration group to allow configuration data to be inherited by any object that matches a wildcard expression.

The configuration group mechanism is separate from the grouping mechanisms used elsewhere in the configuration, such as BGP groups. Configuration groups provide a generic mechanism that can be used throughout the configuration but that are known only to the Junos OS CLI. The individual software processes that perform the actions directed by the configuration receive the expanded form of the configuration—they have no knowledge of configuration groups.

Inheritance Model

Configuration groups use true inheritance, which involves a dynamic, ongoing relationship between the source of the configuration data and the target of that data. Data values changed in the configuration group are automatically inherited by the target. The target does not need to contain the inherited information, although the inherited values can be overridden in the target without affecting the source from which they were inherited.

This inheritance model allows you to see only the instance-specific information without seeing the inherited details. A command pipe in configuration mode allows you to display the inherited data.

Configuring Configuration Groups

For areas of your configuration to inherit configuration statements, you must first put the statements into a configuration group and then apply that group to the levels in the configuration hierarchy that require the statements.

To configure configuration groups and inheritance, you can include the **groups** statement at the **[edit]** hierarchy level:

```
[edit]
groups {
  group-name {
    configuration-data;
  }
}
```

Include the **apply-groups [group-names]** statement anywhere in the configuration where the configuration statements contained in a configuration group are needed.

**Related
Documentation**

- [Creating a Junos OS Configuration Group on page 615](#)

Creating the Junos OS Configuration Group

To create a configuration group, include the **groups** statement at the **[edit]** hierarchy level:

```
[edit]
groups {
  group-name {
    configuration-data;
  }
  lccn-re0 {
    configuration-data;
  }
  lccn-re1 {
    configuration-data;
  }
}
```

group-name is the name of a configuration group. You can configure more than one configuration group by specifying multiple **group-name** statements. However, you cannot use the prefix **junos-** in a group name because it is reserved for use by Junos OS. Similarly, the configuration group **juniper-ais** is reserved exclusively for Juniper Advanced Insight Solutions (AIS)-related configuration. For more information on the **juniper-ais** configuration group, see the [Juniper Networks Advanced Insight Solutions Guide](#).

One reason for the naming restriction is a configuration group called **junos-defaults**. This preset configuration group is applied to the configuration automatically. You cannot modify or remove the **junos-defaults** configuration group. For more information about the Junos default configuration group, see [“Using Junos OS Defaults Groups” on page 640](#).

On routers that support multiple Routing Engines, you can also specify two special group names:

- **re0**—Configuration statements applied to the Routing Engine in slot 0.
- **re1**—Configuration statements applied to the Routing Engine in slot 1.

The configuration specified in group **re0** is only applied if the current Routing Engine is in slot 0; likewise, the configuration specified in group **re1** is only applied if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each **re0** or **re1** group contains at a minimum the configuration for the hostname and the management interface (**fxp0**). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

In addition, the TX Matrix router supports group names for the Routing Engines in each T640 router attached to the routing matrix. Providing special group names for all Routing Engines in the routing matrix allows you to configure the individual Routing Engines in each T640 router differently. Parameters that are not configured at the **[edit groups]** hierarchy level apply to all Routing Engines in the routing matrix.

configuration-data contains the configuration statements applied elsewhere in the configuration with the **apply-groups** statement. To have a configuration inherit the statements in a configuration group, include the **apply-groups** statement. For information about the **apply-groups** statement, see [“Applying a Junos OS Configuration Group” on page 617](#).

The group names for Routing Engines on the TX Matrix router have the following formats:

- **lccn-re0**—Configuration statements applied to the Routing Engine in slot 0 in a specified T640 router.
- **lccn-re1**—Configuration statements applied to the Routing Engine in slot 1 in a specified T640 router.

n identifies the T640 router and can be from 0 through 3. For example, to configure Routing Engine 1 properties for **lcc3**, you include statements at the **[edit groups lcc3-re1]** hierarchy level. For information about the TX Matrix router and routing matrix, see the *Administration Guide for Security Devices*.



NOTE: The management Ethernet interface used for the TX Matrix Plus router, T1600 routers in a routing matrix, and PTX Series Packet Transport Switches, is **em0**. Junos OS automatically creates the router's management Ethernet interface, **em0**.

Related Documentation

- [Applying a Junos OS Configuration Group on page 617](#)
- [Using Junos OS Defaults Groups on page 640](#)
- [Understanding Junos OS Configuration Groups on page 614](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 620](#)
- [Using Wildcards with Configuration Groups on page 622](#)
- [Example: Configuring Sets of Statements with Configuration Groups on page 625](#)

Applying the Junos OS Configuration Group

To have the Junos OS configuration inherit the statements from a configuration group, include the **apply-groups** statement:

```
apply-groups [ group-names ];
```

If you specify more than one group name, list them in order of inheritance priority. The configuration data in the first group takes priority over the data in subsequent groups.

For routers that support multiple Routing Engines, you can specify **re0** and **re1** group names. The configuration specified in group **re0** is only applied if the current Routing Engine is in slot 0; likewise, the configuration specified in group **re1** is only applied if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each **re0** or **re1** group contains at a minimum the configuration for the hostname and the management interface (**fxp0**). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.



NOTE: The management Ethernet interface used for the TX Matrix Plus router, T1600 routers in a routing matrix, and PTX Series Packet Transport Switches, is **em0**.

You can include only one **apply-groups** statement at each specific level of the configuration hierarchy. The **apply-groups** statement at a specific hierarchy level lists the configuration groups to be added to the containing statement's list of configuration groups.

Values specified at the specific hierarchy level override values inherited from the configuration group.

Groups listed in nested **apply-groups** statements take priority over groups in outer statements. In the following example, the BGP neighbor **10.0.0.1** inherits configuration data from group **one** first, then from groups **two** and **three**. Configuration data in group **one** overrides data in any other group. Data from group **ten** is used only if a statement is not contained in any other group.

```
apply-groups [ eight nine ten ];
protocols {
  apply-groups seven;
  bgp {
    apply-groups [ five six ];
    group some-bgp-group {
      apply-groups four;
      neighbor 10.0.0.1 {
        apply-groups [ one two three ];
      }
    }
  }
}
```

When you configure a group defined for the root level—that is, in the default logical system—you cannot successfully apply that group to a nondefault logical system under the `[edit logical-systems logical-system-name]` hierarchy level. Although the router accepts the commit if you apply the group, the configuration group does not take effect for the nondefault logical system. You can instead create an additional configuration group at the root level and apply it within the logical system. Alternatively, you can modify the original group so that it includes configuration for both the default and nondefault logical system hierarchy levels.

Related Documentation

- [Example: Configuring and Applying Junos OS Configuration Groups on page 618](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 620](#)
- [Creating a Junos OS Configuration Group on page 615](#)
- [Using Wildcards with Configuration Groups on page 622](#)
- [Example: Configuring Sets of Statements with Configuration Groups on page 625](#)

Example: Configuring and Applying Junos OS Configuration Groups

In this example, the SNMP configuration is divided between the group **basic** and the normal configuration hierarchy.

There are a number of advantages to placing the system-specific configuration (SNMP contact) into a configuration group and thus separating it from the normal configuration hierarchy—the user can replace (using the **load replace** command) either section without discarding data from the other.

In addition, setting a contact for a specific box is now possible because the group data would be hidden by the router-specific data.

```
[edit]
groups {
  basic { # User-defined group name
    snmp { # This group contains some SNMP data
      contact "My Engineering Group";
      community BasicAccess {
        authorization read-only;
      }
    }
  }
}
apply-groups basic; # Enable inheritance from group "basic"
snmp { # Some normal (non-group) configuration
  location "West of Nowhere";
}
```

This configuration is equivalent to the following:

```
[edit]
snmp {
  location "West of Nowhere";
  contact "My Engineering Group";
}
```

```
community BasicAccess {
  authorization read-only;
}
}
```

For information about how to disable inheritance of a configuration group, see [“Disabling Inheritance of a Junos OS Configuration Group” on page 620](#).

Related Documentation

- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 619](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 626](#)
- [Example: Configuring Peer Entities on page 630](#)
- [Example: Referencing the Preset Statement From the Junos OS defaults Group on page 634](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 635](#)
- [Example: Configuring Sets of Statements with Configuration Groups on page 625](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 628](#)
- [Creating a Junos OS Configuration Group on page 615](#)

Example: Creating and Applying Configuration Groups on a TX Matrix Router

The following example shows how to configure and apply configuration groups on a TX Matrix Router:

```
[edit]
groups {
  re0 { # Routing Engine 0 on TX Matrix router
    system {
      host-name hostname;
      backup-router ip-address;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address ip-address;
          }
        }
      }
    }
  }
  re1 { # Routing Engine 1 on TX Matrix router
    system {
      host-name hostname;
      backup-router ip-address;
    }
    interfaces {
      fxp0 {
        unit 0 {
```

```
        family inet {
            address ip-address;
        }
    }
}
}
lcc0-re0 { # Routing Engine 0 on T640 router numbered 0
    system {
        host-name hostname;
        backup-router ip-address;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address ip-address;
                }
            }
        }
    }
}
lcc0-re1 { # Routing Engine 1 on T640 router numbered 0
    system {
        host-name hostname;
        backup-router ip-address;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address ip-address;
                }
            }
        }
    }
}
}
apply-groups [ re0 re1 lcc0-re0 lcc0-re1 ];
```

- Related Documentation**
- [Example: Configuring and Applying Junos OS Configuration Groups on page 618](#)
 - [Creating a Junos OS Configuration Group on page 615](#)

Disabling Inheritance of a Junos OS Configuration Group

To disable inheritance of a configuration group at any level except the top level of the hierarchy, include the **apply-groups-except** statement:

```
apply-groups-except [ group-names ];
```

This statement is useful when you use the **apply-group** statement at a specific hierarchy level but also want to override the values inherited from the configuration group for a specific parameter.

Example: Disabling Inheritance on Interface so-1/1/0

In the following example, the **apply-groups** statement is applied globally at the interfaces level. The **apply-groups-except** statement is also applied at interface **so-1/1/0** so that it uses the default values for the **hold-time** and **link-mode** statements.

```
[edit]
groups { # "groups" is a top-level statement
  global { # User-defined group name
    interfaces {
      <*> {
        hold-time down 640;
        link-mode full-duplex;
      }
    }
  }
}
apply-groups global;
interfaces {
  so-1/1/0 {
    apply-groups-except global; # Disables inheritance from group "global"
    # so-1/1/0 uses default value for "hold-time"
    # and "link-mode"
  }
}
```

For information about applying a configuration group, see [“Applying a Junos OS Configuration Group” on page 617](#).

Configuration groups can add some confusion regarding the actual values used by the router, because configuration data can be inherited from configuration groups. To view the actual values used by the router, use the **display inheritance** command after the pipe (|) in a **show** command. This command displays the inherited statements at the level at which they are inherited and the group from which they have been inherited.

```
[edit]
user@host# show | display inheritance
snmp {
  location "West of Nowhere";
  ##
  ## 'My Engineering Group' was inherited from group 'basic'
  ##
  contact "My Engineering Group";
  ##
  ## 'BasicAccess' was inherited from group 'basic'
  ##
  community BasicAccess {
    ##
    ## 'read-only' was inherited from group 'basic'
    ##
    authorization read-only;
  }
}
```

To display the expanded configuration (the configuration, including the inherited statements) without the **##** lines, use the **except** command after the pipe in a **show** command:

```
[edit]
user@host# show | display inheritance | except ##
snmp {
  location "West of Nowhere";
  contact "My Engineering Group";
  community BasicAccess {
    authorization read-only;
  }
}
```



NOTE: Using the `display inheritance | except ##` option removes all the lines with `##`. Therefore, you might also not be able to view information about passwords and other important data where `##` is used. To view the complete configuration details with all the information without just the comments marked with `##`, use the `no-comments` option with the `display inheritance` command:

```
[edit]
user@host# show | display inheritance no-comments
snmp {
  location "West of Nowhere";
  contact "My Engineering Group";
  community BasicAccess {
    authorization read-only;
  }
}
```

Related Documentation

- [Applying a Junos OS Configuration Group on page 617](#)
- [Understanding Junos OS Configuration Groups on page 614](#)

Using Wildcards with Configuration Groups

You can use wildcards to identify names and allow one statement to provide data for a variety of statements. For example, grouping the configuration of the **sonet-options** statement over all SONET/SDH interfaces or the dead interval for OSPF over all Asynchronous Transfer Mode (ATM) interfaces simplifies configuration files and eases their maintenance.

Using wildcards in normal configuration data is done in a style that is consistent with that used with traditional UNIX shell wildcards. In this style, you can use the following metacharacters:

- Asterisk (`*`)—Matches any string of characters.
- Question mark (`?`)—Matches any single character.
- Open bracket (`[`)—Introduces a character class.
- Close bracket (`]`)—Indicates the end of a character class. If the close bracket is missing, the open bracket matches a `[` rather than introduce a character class.

- A character class matches any of the characters between the square brackets. Within a configuration group, an interface name that includes a character class must be enclosed in quotation marks.
- Hyphen (-)—Specifies a range of characters.
- Exclamation point (!)—The character class can be complemented by making an exclamation point the first character of the character class. To include a close bracket (]) in a character class, make it the first character listed (after the !, if any). To include a minus sign, make it the first or last character listed.

Wildcarding in configuration groups follows the same rules, but any term using a wildcard pattern must be enclosed in angle brackets *<pattern>* to differentiate it from other wildcarding in the configuration file.

```
[edit]
groups {
  sonet-default {
    interfaces {
      <so-*> {
        sonet-options {
          payload-scrambler;
          rfc-2615;
        }
      }
    }
  }
}
```

Wildcard expressions match (and provide configuration data for) existing statements in the configuration that match their expression only. In the previous example, the expression *<so-*>* passes its **sonet-options** statement to any interface that matches the expression *so-**.

The following example shows how to specify a range of interfaces:

```
[edit]
groups {
  gigabit-ethernet-interfaces {
    interfaces {
      "<ge-1/2/[5-8]>" {
        description "These interfaces reserved for Customer ABC";
      }
    }
  }
}
```

Angle brackets allow you to pass normal wildcarding through without modification. In any matching within the configuration, whether it is done with or without wildcards, the first item encountered in the configuration that matches is used. In the following example, data from the wildcarded BGP groups is inherited in the order in which the groups are listed. The preference value from *<*a*>* overrides the preference in *<*b*>*, just as the **p** value from *<*c*>* overrides the one from *<*d*>*. Data values from any of these groups override the data values from **abcd**.

```
[edit]
user@host# show
groups {
  one {
    protocols {
      bgp {
        group <*a*> {
          preference 1;
        }
        group <*b*> {
          preference 2;
        }
        group <*c*> {
          out-delay 3;
        }
        group <*d*> {
          out-delay 4;
        }
        group abcd {
          preference 10;
          hold-time 10;
          out-delay 10;
        }
      }
    }
  }
}
protocols {
  bgp {
    group abcd {
      apply-groups one;
    }
  }
}
[edit]
user@host# show | display inheritance
protocols {
  bgp {
    group abcd {
      ##
      ## '1' was inherited from group 'one'
      ##
      preference 1;
      ##
      ## '10' was inherited from group 'one'
      ##
      hold-time 10;
      ##
      ## '3' was inherited from group 'one'
      ##
      out-delay 3;
    }
  }
}
```


- Related Documentation**
- [Configuring Wildcard Configuration Group Names on page 633](#)
 - [Applying a Junos OS Configuration Group on page 617](#)
 - [Creating a Junos OS Configuration Group on page 615](#)
 - [Understanding Junos OS Configuration Groups on page 614](#)

Example: Configuring Sets of Statements with Configuration Groups

When sets of statements exist in configuration groups, all values are inherited. For example:

```
[edit]
user@host# show
groups {
  basic {
    snmp {
      interface so-1/1/1.0;
    }
  }
}
apply-groups basic;
snmp {
  interface so-0/0/0.0;
}
[edit]
user@host# show | display inheritance
snmp {
  ##
  ## 'so-1/1/1.0' was inherited from group 'basic'
  ##
  interface [ so-0/0/0.0 so-1/1/1.0 ];
}
```

For sets that are not displayed within brackets, all values are also inherited. For example:

```
[edit]
user@host# show
groups {
  worldwide {
    system {
      name-server {
        10.0.0.100;
        10.0.0.200;
      }
    }
  }
}
apply-groups worldwide;
system {
  name-server {
    10.0.0.1;
    10.0.0.2;
  }
}
```

```
}
[edit]
user@host# show | display inheritance
system {
  name-server {
    ##
    ## '10.0.0.100' was inherited from group 'worldwide'
    ##
    10.0.0.100;
    ##
    ## '10.0.0.200' was inherited from group 'worldwide'
    ##
    10.0.0.200;
    10.0.0.1;
    10.0.0.2;
  }
}
```

- Related Documentation**
- [Understanding Junos OS Configuration Groups on page 614](#)
 - [Creating a Junos OS Configuration Group on page 615](#)
 - [Applying a Junos OS Configuration Group on page 617](#)

Example: Configuring Interfaces Using Junos OS Configuration Groups

You can use configuration groups to separate the common interface media parameters from the interface-specific addressing information. The following example places configuration data for ATM interfaces into a group called **atm-options**:

```
[edit]
user@host# show
groups {
  atm-options {
    interfaces {
      <at-*> {
        atm-options {
          vpi 0 maximum-vcs 1024;
        }
        unit <*> {
          encapsulation atm-snap;
          point-to-point;
          family iso;
        }
      }
    }
  }
}
apply-groups atm-options;
interfaces {
  at-0/0/0 {
    unit 100 {
      vci 0.100;
      family inet {
        address 10.0.0.100/30;
      }
    }
  }
}
```

```

    }
  }
  unit 200 {
    vci 0.200;
    family inet {
      address 10.0.0.200/30;
    }
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  at-0/0/0 {
    ##
    ## "atm-options" was inherited from group "atm-options"
    ##
    atm-options {
      ##
      ## "1024" was inherited from group "atm-options"
      ##
      vpi 0 maximum-vcs 1024;
    }
    unit 100 {
      ##
      ## "atm-snap" was inherited from group "atm-options"
      ##
      encapsulation atm-snap;
      ##
      ## "point-to-point" was inherited from group "atm-options"
      ##
      point-to-point;
      vci 0.100;
      family inet {
        address 10.0.0.100/30;
      }
      ##
      ## "iso" was inherited from group "atm-options"
      ##
      family iso;
    }
    unit 200 {
      ##
      ## "atm-snap" was inherited from group "atm-options"
      ##
      encapsulation atm-snap;
      ##
      ## "point-to-point" was inherited from group "atm-options"
      ##
      point-to-point;
      vci 0.200;
      family inet {
        address 10.0.0.200/30;
      }
      ##
      ## "iso" was inherited from group "atm-options"
    }
  }
}

```

```
        ##
        family iso;
    }
}
[edit]
user@host# show | display inheritance | except ##
interfaces {
  at-0/0/0 {
    atm-options {
      vpi 0 maximum-vcs 1024;
    }
    unit 100 {
      encapsulation atm-snap;
      point-to-point;
      vci 0.100;
      family inet {
        address 10.0.0.100/30;
      }
      family iso;
    }
    unit 200 {
      encapsulation atm-snap;
      point-to-point;
      vci 0.200;
      family inet {
        address 10.0.0.200/30;
      }
      family iso;
    }
  }
}
```

Related Documentation

- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating a Junos OS Configuration Group on page 615](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 572](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 628](#)

Example: Configuring a Consistent IP Address for the Management Interface

On routers with multiple Routing Engines, each Routing Engine is configured with a separate IP address for the management interface (**fxp0**). To access the master Routing Engine, you must know which Routing Engine is active and use the appropriate IP address.

Optionally, for consistent access to the master Routing Engine, you can configure an additional IP address and use this address for the management interface regardless of which Routing Engine is active. This additional IP address is active only on the management interface for the master Routing Engine. During switchover, the address moves to the new master Routing Engine.

In the following example, address **10.17.40.131** is configured for both Routing Engines and includes a **master-only** statement. With this configuration, the **10.17.40.131** address is active only on the master Routing Engine. The address remains consistent regardless of which Routing Engine is active. Address **10.17.40.132** is assigned to **fxp0** on **re0**, and **10.17.40.133** is assigned to **fxp0** on **re1**.

```
[edit groups re0 interfaces fxp0]
unit 0 {
  family inet {
    address 10.17.40.131/25 {
      master-only;
    }
    address 10.17.40.132/25;
  }
}
[edit groups re1 interfaces fxp0]
unit 0 {
  family inet {
    address 10.17.40.131/25 {
      master-only;
    }
    address 10.17.40.133/25;
  }
}
```

This feature is available on all routers that include dual Routing Engines. On a routing matrix composed of the TX Matrix router, this feature is applicable to the switch-card chassis (SCC) only. Likewise, on a routing matrix composed of a TX Matrix Plus router, this feature is applicable to the switch-fabric chassis (SFC) only.



NOTE:

- If you configure the same IP address for a management interface or internal interface such as **fxp0** and an external physical interface such as **ge-0/0/1**, when graceful Routing Engine switchover (GRES) is enabled, the CLI displays an appropriate commit error message that identical addresses have been found on the private and public interfaces. In such cases, you must assign unique IP addresses for the two interfaces that have duplicate addresses.
- The management Ethernet interface used for the TX Matrix Plus router, T1600 routers in a routing matrix, and PTX Series Packet Transport Routers, is **em0**. Junos OS automatically creates the router's management Ethernet interface, **em0**.

Related Documentation

- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating a Junos OS Configuration Group on page 615](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 626](#)

Example: Configuring Peer Entities

In this example, we create a group **some-isp** that contains configuration data relating to another Internet service provider (ISP). We can then insert **apply-group** statements at any point to allow any location in the configuration hierarchy to inherit this data.

```
[edit]
user@host# show
groups {
  some-isp {
    interfaces {
      <xe-*> {
        gigether-options {
          flow-control;
        }
      }
    }
    protocols {
      bgp {
        group <*> {
          neighbor <*> {
            remove-private;
          }
        }
      }
      pim {
        interface <*> {
          version 1;
        }
      }
    }
  }
}
interfaces {
  xe-0/0/0 {
    apply-groups some-isp;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
protocols {
  bgp {
    group main {
      neighbor 10.254.0.1 {
        apply-groups some-isp;
      }
    }
  }
  pim {
    interface xe-0/0/0.0 {
      apply-groups some-isp;
    }
  }
}
```

```

    }
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  xe-0/0/0 {
    ##
    ## "gigether-options" was inherited from group "some-isp"
    ##
    gigether-options {
      ##
      ## "flow-control" was inherited from group "some-isp"
      ##
      flow-control;
    }
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
protocols {
  bgp {
    group main {
      neighbor 10.254.0.1 {
        ##
        ## "remove-private" was inherited from group "some-isp"
        ##
        remove-private;
      }
    }
  }
  pim {
    interface xe-0/0/0.0 {
      ##
      ## "1" was inherited from group "some-isp"
      ##
      version 1;
    }
  }
}

```

Related Documentation

- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating a Junos OS Configuration Group on page 615](#)
- [Establishing Regional Configurations on page 631](#)

Establishing Regional Configurations

In this example, one group is populated with configuration data that is standard throughout the company, while another group contains regional deviations from this standard:

```
[edit]
user@host# show
groups {
  standard {
    interfaces {
      <t3-*> {
        t3-options {
          compatibility-mode larscom subrate 10;
          idle-cycle-flag ones;
        }
      }
    }
  }
  northwest {
    interfaces {
      <t3-*> {
        t3-options {
          long-buildout;
          compatibility-mode kentrox;
        }
      }
    }
  }
}
apply-groups standard;
interfaces {
  t3-0/0/0 {
    apply-groups northwest;
  }
}
[edit]
user@host# show | display inheritance
interfaces {
  t3-0/0/0 {
    ##
    ## "t3-options" was inherited from group "northwest"
    ##
    t3-options {
      ##
      ## "long-buildout" was inherited from group "northwest"
      ##
      long-buildout;
      ##
      ## "kentrox" was inherited from group "northwest"
      ##
      compatibility-mode kentrox;
      ##
      ## "ones" was inherited from group "standard"
      ##
      idle-cycle-flag ones;
    }
  }
}
```


- Related Documentation**
- [Understanding Junos OS Configuration Groups on page 614](#)
 - [Example: Configuring Peer Entities on page 630](#)

Configuring Wildcard Configuration Group Names

Wildcards are configuration group names that use special characters to create a pattern that can be applied to multiple statements. Wildcards are useful for copying one set of configuration options to a large number of different configuration groups. It is important to set up your wildcard name properly to ensure that the wildcard configuration options get copied to the appropriate configuration groups.

In this example, you configure different values for the `<*-major>` and `<*-minor>` wildcard groups under the `label-switched-path` statement. The asterisk (*) character represents a section of the wildcard name that can match any string of characters. For example the configuration options under `label-switched-path <*-major>` are passed onto `label-switched-path metro-major` and any other `label-switched-path` configuration group containing `-major` in its name.

```
[edit]
user@host# show
groups {
  mpls-conf {
    protocols {
      mpls {
        label-switched-path <*-major> {
          retry-timer 5;
          bandwidth 155m;
          optimize-timer 60;
        }
        label-switched-path <*-minor> {
          retry-timer 15;
          bandwidth 64k;
          optimize-timer 120;
        }
      }
    }
  }
}
apply-groups mpls-conf;
protocols {
  mpls {
    label-switched-path metro-major {
      to 10.0.0.10;
    }
    label-switched-path remote-minor {
      to 10.0.0.20;
    }
  }
}
[edit]
user@host# show | display inheritance
protocols {
```

```

mpls {
  label-switched-path metro-major {
    to 10.0.0.10;
    ##
    ## "5" was inherited from group "mpls-conf"
    ##
    retry-timer 5;
    ## "155m" was inherited from group "mpls-conf"
    ##
    bandwidth 155m;
    ##
    ## "60" was inherited from group "mpls-conf"
    ##
    optimize-timer 60;
  }
  label-switched-path remote-minor {
    to 10.0.0.20;
    ##
    ## "15" was inherited from group "mpls-conf"
    ##
    retry-timer 15;
    ##
    ## "64k" was inherited from group "mpls-conf"
    ##
    bandwidth 64k;
    ##
    ## "120" was inherited from group "mpls-conf"
    ##
    optimize-timer 120;
  }
}

```

Related Documentation

- [Using Wildcards with Configuration Groups on page 622](#)

Example: Referencing the Preset Statement From the Junos OS defaults Group

The following example is a preset statement from the Junos defaults group that is available for FTP in a stateful firewall:

```

[edit]
groups {
  junos-defaults {
    applications {
      application junos-ftp {# Use FTP default configuration
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
      }
    }
  }
}

```

To reference a preset Junos default statement from the Junos defaults group, include the **junos-default-name** statement at the applicable hierarchy level. For example, to

reference the Junos default statement for FTP in a stateful firewall, include the **junos-ftp** statement at the **[edit services stateful-firewall rule my-rule term my-term from applications]** hierarchy level:

```
[edit]
services {
  stateful-firewall {
    rule my-rule {
      term my-term {
        from {
          applications junos-ftp; #Reference predefined statement, junos-ftp
        }
      }
    }
  }
}
```

Related Documentation

- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 635](#)
- [Using Junos OS Defaults Groups on page 640](#)
- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating a Junos OS Configuration Group on page 615](#)

Example: Viewing Default Statements That Have Been Applied to the Configuration

To view the Junos defaults that have been applied to the configuration, issue the **show | display inheritance defaults** command. For example, to view the inherited Junos defaults at the **[edit system ports]** hierarchy level:

```
user@host# show system ports | display inheritance defaults
## ## 'console' was inherited from group 'junos-defaults'
## 'vt100' was inherited from group 'junos-defaults'
## console type vt100;
```

If you choose not to use existing Junos default statements, you can create your own configuration groups manually.

To view the complete configuration information without the comments marked with **##**, use the **no-comments** option with the **display inheritance** command.

Related Documentation

- [Creating a Junos OS Configuration Group on page 615](#)
- [Configuring Configuration Groups on page 614](#)

Using Conditions to Apply Configuration Groups Overview

You can use the **when** statement at the **[edit groups group-name]** hierarchy level to define conditions under which a configuration group should be applied.

You can configure a group to be applied based on the type of chassis, model, or Routing Engine, virtual chassis member, cluster node, and start and optional end time of day or date.

For example, you could use the **when** statement to create a generic configuration group for each type of node and then apply the configuration based on certain node properties, such as chassis or model.

Related Documentation

- [Example: Configuring Conditions for Applying Configuration Groups on page 636](#)

Example: Configuring Conditions for Applying Configuration Groups

This example shows how to configure conditions under which a specified configuration group is to be applied.

- [Requirements on page 636](#)
- [Overview on page 636](#)
- [Configuration on page 637](#)

Requirements

No special configuration beyond device initialization is required before you configure this example.

Overview

You can configure your group configuration data at the **[edit groups group-name]** hierarchy level, then use the **when** statement to have the group applied based on conditions including: type of chassis, model, routing-engine, virtual chassis member, cluster node, and start and optional end time of day or date.

If you specify multiple conditions in a single configuration group, all conditions must be met before the configuration group is applied.

You can specify the start time or the time duration for the configuration group to be applied. If only the start time is specified, the configuration group is applied at the specified time and it remains in effect until the time is changed. If the end time is specified, then on each day, the applied configuration group is started and stopped at the specified times.

This example sets conditions in a configuration group, **test1**, such that this group is applied only when all of the following conditions are met: the router is a model MX240 router with chassis type LCC0, with a Routing Engine operating as RE0, is member0 of the virtual

chassis on node0, and the configuration group will only be in effect from 9:00 a.m. until 5:00 p.m. each day.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set groups test1 when model mx240
set groups test1 when chassis lcc0
set groups test1 when routing-engine re0
set groups test1 when member member0
set groups test1 when node node0
set groups test1 when time 9 to 5
```

Step-by-Step Procedure To configure conditions for configuration group **test1**:

1. Set the condition that identifies the model MX240 router.

```
[edit groups test1 when]
user@host# set model mx240
```
2. Set the condition that identifies the chassis type as LCC0.

```
[edit groups test1 when]
user@host# set chassis lcc0
```
3. Set the condition that identifies the Routing Engine operating as RE0.

```
[edit groups test1 when]
user@host# set routing-engine re0
```
4. Set the condition that identifies the virtual chassis **member0**.

```
[edit groups test1 when]
user@host# set member member0
```
5. Set the condition that identifies the cluster **node0**.

```
[edit groups test1 when]
user@host# set node node0
```
6. Set the condition that applies the group only between the hours of 9:00 a.m. and 5:00 p.m. daily.

```
[edit groups test1 when]
user@host# set time 9 to 5
```



NOTE: The syntax for specifying the time is: `time <start-time> [to <end-time>]` using the time format `yyyy-mm-dd.hh:mm`, `hh:mm`, or `hh`.

7. Commit the configuration.

```
user@host# commit
```

Results From configuration mode, confirm your configuration by entering the **show groups test1** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show groups test1
when {
  time 9 to 5;
  chassis lcc0;
  model mx240;
  routing-engine re0;
  member member0;
  node node0;
}
```

Verification

Confirm that the configuration is working properly.

- [Checking Group Inheritance with Conditional Data on page 638](#)

Checking Group Inheritance with Conditional Data

Purpose Verify that conditional data from a configuration group is inherited when applied.

Action The **show | display inheritance** operational command can be issued with the **when** data to display the conditional inheritance. Using this example, you could issue one of these commands to determine that the conditional data was inherited:

```
user@host> show | display inheritance when model mx240
user@host> show | display inheritance when chassis lcc0
user@host> show | display inheritance when routing-engine re0
user@host> show | display inheritance when member member0
user@host> show | display inheritance when node node0
user@host> show | display inheritance when time 9 to 5
```

**Related
Documentation**

- [Understanding Junos OS Configuration Groups on page 614](#)
- [Creating a Junos OS Configuration Group on page 615](#)
- [Applying a Junos OS Configuration Group on page 617](#)
- [Using Conditions to Apply Configuration Groups Overview on page 636](#)

Improving Commit Time When Using Configuration Groups

Configuration groups are used for applying configurations across other hierarchies without re-entering configuration data. Some configuration groups specify every configuration detail. Other configuration groups make use of wildcards to configure ranges of data, without detailing each configuration line. Some configurations have an inheritance path that includes a long string of configurations to be applied.

When a configuration that uses configuration groups is committed, the commit process expands and reads all of the configuration data of the group into memory in order to

apply the configurations as intended. The commit performance can be negatively impacted if many configuration groups are being applied, especially if the configuration groups use wildcards extensively.

If your system uses many configuration groups that use wildcards, you can configure the **persist-groups-inheritance** statement at the **[edit system commit]** hierarchy level to improve commit time performance.

Using this option allows the system to build the inheritance path for each configuration group inside the database, instead of in the process memory. This can improve commit time performance. However, it can also increase the database size by up to 22 percent.

**Related
Documentation**

- [Example: Improving Commit Time When Using Configuration Groups on page 639](#)
- *persist-groups-inheritance*

Example: Improving Commit Time When Using Configuration Groups

This example shows how to use the **persist-groups-inheritance** configuration statement to improve commit time performance when committing configurations that make use of many configuration groups that are created using wildcards.

- [Requirements on page 639](#)
- [Overview on page 639](#)
- [Configuration on page 640](#)
- [Verification on page 640](#)

Requirements

This example uses the following hardware and software components:

- One Juniper Networks M Series, MX Series, or T Series router that uses a number of configuration groups created with wildcards.
- Junos OS Release 13.2 or later.

Overview

When committing a configuration that uses configuration groups, at the time of commit, all of the inheritance paths of the configuration groups must be fully expanded into memory to apply the configurations as intended. This can negatively impact commit performance if there are many configuration groups and they are configured using wildcards.

To improve commit performance, you can configure **persist-groups-inheritance** at the **[edit system commit]** hierarchy level. Configuring this option causes the configuration groups to be expanded into the database instead of into the process memory at commit time.

Configuration

Configuring Persist Groups Inheritance

Step-by-Step Procedure

To configure **persist-groups-inheritance**:

1. Set the **persist-groups-inheritance** option.

```
[edit system commit]  
user@host# set persist-groups-inheritance
```
2. Commit the configuration.

```
[edit system commit]  
user@host# commit
```

Verification

Verifying the Configuration

Purpose Verify that **persist-groups-inheritance** is configured.

Action To confirm the configuration, use the **show system commit** command.

```
[edit ]  
user@host# show system commit  
persist-groups-inheritance
```

Related Documentation

- [Improving Commit Time When Using Configuration Groups on page 638](#)
- *persist-groups-inheritance*

Using Junos OS Defaults Groups

Junos OS provides a hidden and immutable configuration group called **junos-defaults** that is automatically applied to the configuration of your router. The **junos-defaults** group contains preconfigured statements that contain predefined values for common applications. Some of the statements must be referenced to take effect, such as definitions for applications (for example, FTP or telnet settings). Other statements are applied automatically, such as terminal settings.



NOTE: Many identifiers included in the **junos-defaults** configuration group begin with the name **junos-**. Because identifiers beginning with the name **junos-** are reserved for use by Juniper Networks, you cannot define any configuration objects using this name.

You cannot include **junos-defaults** as a configuration group name in an **apply-groups** statement.

To view the full set of available preset statements from the Junos defaults group, issue the **show groups junos-defaults** configuration mode command at the top level of the configuration. The following example displays a partial list of Junos defaults groups:

```
user@host# show groups junos-defaults
# Make vt100 the default for the console port
system {
  ports {
    console type vt100;
  }
}
applications {
  # File Transfer Protocol
  application junos-ftp {
    application-protocol ftp;
    protocol tcp;
    destination-port 21;
  }
  # Trivial File Transfer Protocol
  application junos-tftp {
    application-protocol tftp;
    protocol udp;
    destination-port 69;
  }
  # RPC port mapper on TCP
  application junos-rpc-portmap-tcp {
    application-protocol rpc-portmap;
    protocol tcp;
    destination-port 111;
  }
  # RPC port mapper on UDP
}
```

To reference statements available from the **junos-defaults** group, include the selected **junos- *default-name*** statement at the applicable hierarchy level.

Related Documentation

- [Creating a Junos OS Configuration Group on page 615](#)
- [Example: Referencing the Preset Statement From the Junos OS defaults Group on page 634](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 635](#)

Set Up Routing Engine Configuration Groups

In a router with two Routing Engines, one configuration should be shared between both Routing Engines. This ensures that both Routing Engine configurations are identical. Within this configuration, create two Routing Engine groups, one for each Routing Engine. Within these groups, you specify the Routing Engine–specific parameters.

For more information about creating configuration groups, see *CLI User Guide*.

For more information about the initial configuration for redundant Routing Engine systems and the re0 group, see *Junos OS High Availability Library for Routing Devices*.

1. Create the configuration group **re0**. The **re0** group is a special group designator that is only used by **RE0** in a redundant routing platform.

```
[edit]
root# set groups re0
```

2. Navigate to the **groups re0** level of the configuration hierarchy.

```
[edit]
root# edit groups re0
```

3. Specify the router hostname.

```
[edit groups re0]
root# set system host-name host-name
```



NOTE: The hostname specified in the router configuration is not used by the DNS server to resolve to the correct IP address. This hostname is used to display the name of the Routing Engine in the CLI. For example, the hostname appears at the command-line prompt when the user is logged in to the CLI:

```
user-name@host-name>
```

4. Configure the IP address and prefix length for the router Ethernet interface.
 - For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces em0 unit 0 family inet address address/prefix-length
```

To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

- For a T1600 standalone router (not connected to a TX Matrix Plus router and not in a routing matrix):

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

5. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

6. Create the configuration group **re1**.

```
[edit]
root# set groups re1
```

7. Navigate to the **groups re1** level of the configuration hierarchy.

```
[edit]
root# edit groups re1
```

8. Specify the router hostname.

```
[edit groups re1]
root# set system host-name host-name
```

9. Configure the IP address and prefix length for the router Ethernet interface.

- For all devices *except* the TX Matrix Plus router, T1600 or T4000 routers in a routing matrix, and PTX Series Packet Transport Routers:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

- For TX Matrix Plus router, and T1600 or T4000 routers in a routing matrix only:

```
[edit]
root@# set interfaces em0 unit 0 family inet address address/prefix-length
```

To use **em0** as an out-of-band management Ethernet interface, you must configure its logical port, **em0.0**, with a valid IP address.

- For a T1600 standalone router (not connected to a TX Matrix Plus router, and not in a routing matrix):

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

10. Return to the top level of the hierarchy.

```
[edit groups re0]
root# top
```

11. Specify the group application order.

```
[edit]
root# set apply-groups [ re0 re1 ]
```


Controlling the CLI Environment

- [Controlling the Junos OS CLI Environment on page 645](#)
- [Setting the Junos OS CLI Screen Length and Width on page 647](#)
- [Example: Controlling the CLI Environment on page 648](#)
- [Example: Enabling Configuration Breadcrumbs on page 654](#)

Controlling the Junos OS CLI Environment

In operational mode, you can control the Junos OS command-line interface (CLI) environment. For example, you can specify the number of lines that are displayed on the screen or your terminal type. The following output lists the options that you can use to control the CLI environment:

```
user@host>set cli ?
Possible completions:
complete-on-space  Set whether typing space completes current word
directory          Set working directory
idle-timeout       Set maximum idle time before login session ends
logical-system     Set default logical system
prompt            Set CLI command prompt string
restart-on-upgrade Set whether CLI prompts to restart after software upgrade

screen-length      Set number of lines on screen
screen-width       Set number of characters on a line
terminal          Set terminal type
timestamp          Timestamp CLI output
```



NOTE: When you use SSH to log in to the router or log in from the console when its terminal type is already configured, your terminal type, screen length, and screen width are already set.

This chapter discusses the following topics:

- [Setting the Terminal Type on page 646](#)
- [Setting the CLI Prompt on page 646](#)
- [Setting the CLI Directory on page 646](#)
- [Setting the CLI Timestamp on page 646](#)

- [Setting the Idle Timeout on page 646](#)
- [Setting the CLI to Prompt After a Software Upgrade on page 646](#)
- [Setting Command Completion on page 647](#)
- [Displaying CLI Settings on page 647](#)

Setting the Terminal Type

To set the terminal type, use the **set cli terminal** command:

```
user@host> set cli terminal terminal-type
```

The terminal type can be one of the following: **ansi**, **vt100**, **small-xterm**, or **xterm**.

Setting the CLI Prompt

The default CLI prompt is **user@host>**. To change this prompt, use the **set cli prompt** command. If the prompt string contains spaces, enclose the string in quotation marks (" ").

```
user@host> set cli prompt string
```

Setting the CLI Directory

To set the current working directory, use the **set cli directory** command:

```
user@host> set cli directory directory
```

directory is the pathname of working directory.

Setting the CLI Timestamp

By default, CLI output does not include a timestamp. To include a timestamp in CLI output, use the **set cli timestamp** command:

```
user@host> set cli timestamp [format time-date-format | disable]
```

If you do not specify a timestamp format, the default format is **Mmm dd hh:mm:ss** (for example, Feb 08 17:20:49). Enclose the format in single quotation marks (').

Setting the Idle Timeout

By default, an individual CLI session never times out after extended times, unless the **idle-timeout** statement has been included in the user's login class configuration. To set the maximum time an individual session can be idle before the user is logged off the router, use the **set cli idle-timeout** command:

```
user@host> set cli idle-timeout timeout
```

timeout can be 0 through 100,000 minutes. Setting **timeout** to 0 disables the timeout.

Setting the CLI to Prompt After a Software Upgrade

By default, the CLI prompts you to restart after a software upgrade. To disable the prompt for an individual session, use the **set cli restart-on-upgrade off** command:

```
user@host> set cli restart-on-upgrade off
```

To reenable the prompt, use the **set cli restart-on-upgrade on** command:

```
user@host> set cli restart-on-upgrade on
```

Setting Command Completion

By default, you can press Tab or the Spacebar to have the CLI complete a command.

To have the CLI allow only a tab to complete a command, use the **set cli complete-on-space off** command:

```
user@host> set cli complete-on-space off
Disabling complete-on-space
user@host>
```

To reenable the use of both spaces and tabs for command completion, use the **set cli complete-on-space on** command:

```
user@host> set cli complete-on-space on
Enabling complete-on-space
user@host>
```

Displaying CLI Settings

To display the current CLI settings, use the **show cli** command:

```
user@host> show cli
CLI screen length set to 24
CLI screen width set to 80
CLI complete-on-space set to on
```



NOTE: In Junos OS Release 13.3 and later, the value of screen width is 0 or in the range of 40 through 1024.

- Related Documentation**
- [Example: Controlling the CLI Environment on page 648](#)

Setting the Junos OS CLI Screen Length and Width

You can set the Junos OS command-line interface (CLI) screen length and width according to your specific requirements. This topic contains the following sections:

- [Setting the Screen Length on page 647](#)
- [Setting the Screen Width on page 648](#)

Setting the Screen Length

The default CLI screen length is 24 lines. To change the length, use the **set cli screen-length** command:

```
user@host> set cli screen-length length
```

Setting the screen length to 0 lines disables the display of output one screen at a time. Disabling this UNIX **more**-type interface can be useful when you are issuing CLI commands from scripts.

Setting the Screen Width

The value of CLI screen width is **0** or in the range of **40** through **1024**. The default CLI screen width is 80 characters. To change the width, use the **set cli screen-width** command:

```
user@host> set cli screen-width width
```



NOTE: In Junos OS Release 13.2 and earlier, the value of *width* is in the range of 0 through 1024.

Related Documentation

- [Example: Controlling the CLI Environment on page 648](#)
- [Controlling the Junos OS CLI Environment on page 645](#)

Example: Controlling the CLI Environment

The following example shows you how to change the default CLI environment.

Changing the CLI environment is all about customizing the CLI window to fit your personal preferences. Use the settings discussed in this topic to make the CLI window look and behave according to what you find most convenient and efficient.

- [Requirements on page 648](#)
- [Overview on page 649](#)
- [Configuration on page 649](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Before starting this example, check what the default settings are. Use the **show cli** operational mode command.

```
user@host> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen length set to 66
CLI screen width set to 80
CLI terminal is 'xterm'
```

Is the prompt set to your *username@routename*? If not, exit the CLI and enter the operational mode again.

Is the CLI screen length set to 66 and the CLI screen width set to 80? If so, you can start the example. Otherwise, make these changes to the CLI settings:


```

user@host> set cli screen-length 66
Screen length set to 66 lines long
user@host> set cli screen-width 80
Screen width set to 80 columns wide

```

Overview

To see a list of CLI environmental settings that you can change, use the **set cli ?** command.

```

user@host> set cli ?
Possible completions:
  complete-on-space  Set whether typing space completes current word
  directory           Set working directory
  idle-timeout        Set maximum idle time before login session ends
  logical-system      Set default logical system
  prompt             Set CLI command prompt string
  restart-on-upgrade  Set whether CLI prompts to restart after software upgrade
  screen-length       Set number of lines on screen
  screen-width        Set number of characters on a line
  terminal            Set terminal type
  timestamp           Timestamp CLI output

```

This example focuses on three of these commands: **set cli screen-length**, **set cli screen-width**, and **set cli prompt**.

Configuration

This configuration example has the following sections:

- [Configuring the CLI Prompt on page 650](#)
- [Configuring CLI Width on page 650](#)
- [Configuring CLI Length on page 651](#)
- [Return to the Default CLI Prompt on page 653](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them in a text file, remove any line breaks, change the values used to match your network configuration, and then copy and paste the commands into the CLI at the operational command prompt.

```

set cli prompt "router1-san-jose> "
set cli screen-width 110
set cli screen-length 45

```



NOTE: In Junos OS Release 13.3 and later, the value of screen width is 0 or in the range of 40 through 1024.

Configuring the CLI Prompt

Step-by-Step Procedure The default CLI prompt is your *username@hostname*. But you can have any prompt you find useful.

To configure a different CLI prompt:

- Use the following operational mode command where *string* is the exact text you want to see at the command line.

```
set cli prompt "string"
```

For example, if "*string*" is "router1-san-jose> ", the command is as follows:

```
set cli prompt "router1-san-jose> "
router1-san-jose>
```

Configuring CLI Width

Step-by-Step Procedure How do you know what width works best for you? This example discusses how CLI width can affect what you see.

To configure a new default CLI width:

- See what the current defaults are for the CLI environment.

```
router1-san-jose> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen length set to 66
CLI screen width set to 80
CLI terminal is 'xterm'
router1-san-jose>
```



NOTE: In Junos OS Release 13.3 and later, the value of *width* is 0 or in the range of 40 through 1024.

- Look at the following output for the operational command **show class-of-service forwarding-class**.

The output from this command is wider than some and so illustrates a common problem with viewing output. If, for example, you have a relatively narrow window, command output might show up in overrun lines.

```
router1-san-jose> show class-of-service forwarding-class
Forwarding class  ID  Queue  Restricted queue  Fabric
priority Policing priority SPU priority
premium-rate      0   0      0                low
normal
medium-rate       1   1      1                low
normal
low-rate          2   2      2                low
normal
```

```

NC          3      3      3      low
normal
tunnel-rate 4      4      0      low
normal

```

The lines look to be intermingled and it is hard to read across to find the information you might be seeking.

3. Change the window width to 110 columns.

Notice how the output of this command is much easier to read in the wider format:

```
router1-san-jose> set cli screen-width 110
```

```
router1-san-jose> show class-of-service forwarding-class
```

Forwarding class	ID	Queue	Restricted queue	Fabric priority	Policing priority	SPU priority
premium-rate	0	0	0	low	normal	low
medium-rate	1	1	1	low	normal	low
low-rate	2	2	2	low	normal	low
NC	3	3	3	low	normal	low
tunnel-rate	4	4	0	low	normal	low

Configuring CLI Length

Step-by-Step Procedure

You can configure the length of the CLI screen in a similar fashion as you did the width.

To configure a new default CLI length:

1. See what the current defaults are for the CLI environment.

```

router1-san-jose> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen length set to 66
CLI screen width set to 80
CLI terminal is 'xterm'
router1-san-jose>

```

2. Look at the following output for the operational command **show version**.

```

Makefile                                sync-dpm-sb.manifest
build                                  sync-equilibrium-sb.manifest
etc                                   sync-equilibrium2-sb.manifest
include                               sync-hellopics-sb.manifest
jexample                             sync-ipprobe-mt-sb.manifest
jnx-cc-routeservice-sb.manifest       sync-ipprobe-sb.manifest
jnx-example-sb.manifest               sync-ipsnooper-sb.manifest
jnx-flow-sb.manifest                  sync-monitube-sb.manifest
jnx-gateway-sb.manifest               sync-monitube2-plugin-sb.manifest
jnx-ifinfo-sb.manifest                sync-packetproc-sb.manifest
jnx-mspexampled-sb.manifest           sync-passthru-sb.manifest
jnx-msprsm-sb.manifest                sync-policy-manager-sb.manifest
jnx-routeservice-sb.manifest          sync-reassembler-sb.manifest
lib                                   sync-route-manager-sb.manifest
JnprFirewall-Proto.html               Makefile.depend.octeon dfw_filter.proto
JnprFirewall.html                     Makefile.depend.powerpc dfw_ifattach.proto
Makefile                             Makefile.depend.xlr   dfw_policer.proto
Makefile.depend.arm                   dfw.jsdl              dfw_stats.proto

```

```
Makefile.depend.host    dfw_bulk.proto
Makefile.depend.i386    dfw_common.proto
```

```
Trying 192.168.184.75...
Connected to spot-fxp0.englab.juniper.net.
Escape character is '^'.
Unauthorized use is prohibited.
```

```
router1-san-jose> show version
Hostname: spot
Model: mx240
Junos: 14.2-20140710_ib_14_2_psd.1
JUNOS Base OS boot [14.2-20140710_ib_14_2_psd.1]
JUNOS Base OS Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Kernel Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Crypto Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Packet Forwarding Engine Support (M/T/EX Common)
[14.2-20140710_ib_14_2_psd.1]
JUNOS Packet Forwarding Engine Support (MX Common)
[14.2-20140710_ib_14_2_psd.1]
JUNOS Online Documentation [14.2-20140710_ib_14_2_psd.1]
JUNOS Services AACL Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Application Level Gateways [14.2-20140710_ib_14_2_psd.1]
JUNOS AppId Services [14.2-20140710_ib_14_2_psd.1]
JUNOS Border Gateway Function package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Captive Portal and Content Delivery Container package
[14.2-20140710_ib_14_2_psd.1]
JUNOS Services HTTP Content Management package [14.2-20140710_ib_14_2_psd.1]
JUNOS IDP Services [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Jflow Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services LL-PDF Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services MobileNext Software package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Mobile Subscriber Service Container package
[14.2-20140710_ib_14_2_psd.1]
JUNOS Services NAT [14.2-20140710_ib_14_2_psd.1]
JUNOS Services PTSP Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services RPM [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Stateful Firewall [14.2-20140710_ib_14_2_psd.1]
JUNOS Voice Services Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Crypto [14.2-20140710_ib_14_2_psd.1]
JUNOS Services SSL [14.2-20140710_ib_14_2_psd.1]
JUNOS Services IPSec [14.2-20140710_ib_14_2_psd.1]
JUNOS platform Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Routing Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Runtime Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Web Management [14.2-20140710_ib_14_2_psd.1]
JUNOS py-base-i386 [14.2-20140710_ib_14_2_psd.1]
```

```
router1-san-jose>
```

The current length is 66 lines, which is close to the length of a typical monitor. But even though the output is fairly long, it hardly needs all that space to be clearly seen in its entirety. In fact, it is harder to pick out just where the output starts in a screen this long.

3. Change the window width to 45 lines.


```
router1-san-jose> set cli screen-length 45
```
4. Now look at the output again.

```

router1-san-jose> show version
Hostname: spot
Model: mx240
Junos: 14.2-20140710_ib_14_2_psd.1
JUNOS Base OS boot [14.2-20140710_ib_14_2_psd.1]
JUNOS Base OS Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Kernel Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Crypto Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Packet Forwarding Engine Support (M/T/EX Common)
[14.2-20140710_ib_14_2_psd.1]
JUNOS Packet Forwarding Engine Support (MX Common)
[14.2-20140710_ib_14_2_psd.1]
JUNOS Online Documentation [14.2-20140710_ib_14_2_psd.1]
JUNOS Services AACL Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Application Level Gateways [14.2-20140710_ib_14_2_psd.1]
JUNOS AppId Services [14.2-20140710_ib_14_2_psd.1]
JUNOS Border Gateway Function package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Captive Portal and Content Delivery Container package
[14.2-20140710_ib_14_2_psd.1]
JUNOS Services HTTP Content Management package [14.2-20140710_ib_14_2_psd.1]
JUNOS IDP Services [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Jflow Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services LL-PDF Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services MobileNext Software package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Mobile Subscriber Service Container package
[14.2-20140710_ib_14_2_psd.1]
JUNOS Services NAT [14.2-20140710_ib_14_2_psd.1]
JUNOS Services PTSP Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services RPM [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Stateful Firewall [14.2-20140710_ib_14_2_psd.1]
JUNOS Voice Services Container package [14.2-20140710_ib_14_2_psd.1]
JUNOS Services Crypto [14.2-20140710_ib_14_2_psd.1]
JUNOS Services SSL [14.2-20140710_ib_14_2_psd.1]
JUNOS Services IPSec [14.2-20140710_ib_14_2_psd.1]
JUNOS platform Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Routing Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Runtime Software Suite [14.2-20140710_ib_14_2_psd.1]
JUNOS Web Management [14.2-20140710_ib_14_2_psd.1]
JUNOS py-base-i386 [14.2-20140710_ib_14_2_psd.1]

router1-san-jose>

```

With a shorter sscreen, you can easily see where the current output begins and ends.

Return to the Default CLI Prompt

Step-by-Step Procedure

To go back to the default prompt:

1. Exit the CLI.

```

router1-san-jose> exit
%

```
2. Enter the CLI operational mode again.

```

% cli
user@host>

```

- Related Documentation**
- [Setting the Junos OS CLI Screen Length and Width on page 647](#)
 - [Controlling the Junos OS CLI Environment on page 645](#)

Example: Enabling Configuration Breadcrumbs

The output of **show configuration** operational mode command and **show configuration** mode commands can be configured to display configuration breadcrumbs that indicate the exact location in the hierarchy of the output being viewed.

Before enabling the configuration breadcrumbs feature, check the output of the **show configuration** command.

```
user@host> show configuration
```

```
...
    }
  }
}
fe-4/1/2 {
  description "FA4/1/2: mxvj1-mr6 (64.12.137.160/27) (T=bb1an, bbmail,
bbowmtc)";
  unit 0 {
    family inet {
      filter {
        output 151mj;
      }
      address 64.12.137.187/27 {
        vrrp-group 1 {
          virtual-address 64.12.137.189;
        }
      }
    }
  }
}
---(more 18%)-----
```

In the output, there is no clear indication about the section of the configuration being viewed.

To enable the configuration breadcrumbs feature:

1. Define a class at the **[edit system login]** hierarchy level.

```
[edit system login]
user@host# set class breadclass idle-timeout 10
```

2. Add a user to the defined login class to enable the breadcrumbs output view when this user enters the **show configuration** operational mode command.

```
[edit system login user user1]
user@host# set class breadclass
```

3. Configure the **configuration-breadcrumbs** statement at the **[edit system login class <class name>]** hierarchy level.

```
[edit system login class breadclass]
user@host# set configuration-breadcrumbs
```

4. Confirm the configuration.

```
[edit]
user@host# commit
```

On enabling configuration breadcrumbs in the CLI, User1 (the user added to the login class) can verify the feature in the output by entering the **show configuration** command.

```
user1@host> show configuration
```

```
...
    }
  }
}
fe-4/1/2 {
  description "FA4/1/2: mxvj1-mr6 (64.12.137.160/27) (T=bb1an, bbmail,
bbowmtc)";
  unit 0 {
    family inet {
      filter {
        output 151mj;
      }
      address 64.12.137.187/27 {
        vrrp-group 1 {
          virtual-address 64.12.137.189;
---(more 18%)---[groups main interfaces fe-4/1/2 unit 0 family inet address
64.12.137.187/27 vrrp-group 1]---
```

The new output indicates the exact location of the configuration hierarchy being viewed. User1 is currently viewing the interface configuration of a group.



NOTE: If you are enabling configuration breadcrumbs for your own user account, you should log out and log in again to see the changes.

- Related Documentation**
- [class](#)
 - [configuration-breadcrumbs on page 668](#)

CHAPTER 30

Junos OS Configuration Statements and Commands

- [apply-groups on page 658](#)
- [apply-groups-except on page 659](#)
- [activate](#)
- [annotate](#)
- [commit](#)
- [commit-interval \(Batch Commits\) on page 667](#)
- [configuration-breadcrumbs on page 668](#)
- [copy](#)
- [days-to-keep-error-logs \(Batch Commits\) on page 669](#)
- [deactivate](#)
- [delete](#)
- [edit](#)
- [exit](#)
- [groups on page 674](#)
- [help](#)
- [insert](#)
- [load](#)
- [maximum-aggregate-pool \(Batch Commits\) on page 679](#)
- [maximum-entries \(Batch Commits\) on page 680](#)
- [protect](#)
- [quit](#)
- [rename](#)
- [replace](#)
- [rollback](#)
- [run](#)
- [save](#)

- [server \(Batch Commits\) on page 688](#)
- [set](#)
- [show](#)
- [show configuration](#)
- [show | display inheritance](#)
- [show | display omit](#)
- [show | display set](#)
- [show | display set relative](#)
- [show groups junos-defaults](#)
- [status](#)
- [top](#)
- [traceoptions \(Batch Commits\) on page 701](#)
- [unprotect](#)
- [up](#)
- [update](#)
- [when on page 705](#)
- [wildcard delete](#)

apply-groups

Syntax	<code>apply-groups [<i>group-names</i>];</code>
Hierarchy Level	All hierarchy levels
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Apply a configuration group to a specific hierarchy level in a configuration, to have a configuration inherit the statements in the configuration group.</p> <p>You can specify more than one group name. You must list them in order of inheritance priority. The configuration data in the first group takes priority over the data in subsequent groups.</p>
Options	<i>group-names</i> —One or more names specified in the groups statement.
Required Privilege Level	<code>configure</code> —To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Applying a Junos OS Configuration Group on page 617• groups on page 674

apply-groups-except

Syntax	<code>apply-groups-except [<i>group-names</i>];</code>
Hierarchy Level	All hierarchy levels except the top level
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Disable inheritance of a configuration group.
Options	<i>group-names</i> —One or more names specified in the groups statement.
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• groups on page 674• Disabling Inheritance of a Junos OS Configuration Group on page 620

activate

Syntax	<code>activate (<i>statement</i> <i>identifier</i>)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Remove the inactive: tag from a statement, effectively adding the statement or identifier back to the configuration. Statements or identifiers that have been activated take effect when you next issue the commit command.
Options	<p><i>identifier</i>—Identifier from which you are removing the inactive tag. It must be an identifier at the current hierarchy level.</p> <p><i>statement</i>—Statement from which you are removing the inactive tag. It must be a statement at the current hierarchy level.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• deactivate on page 670• Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489

annotate

Syntax `annotate statement "comment-string"`

Release Information Command introduced before Junos OS Release 7.4.

Description Add comments to a configuration. You can add comments only at the current hierarchy level.

Any comments you add appear only when you view the configuration by entering the [show](#) command in configuration mode or the **show configuration** command in operational mode.



NOTE: The Junos OS supports annotation up to the last level in the configuration hierarchy, including oneliners. However, annotation of parts (child statements or identifiers within a oneliner) of the oneliner is not supported. For example, in the following sample configuration hierarchy, annotation is supported up to the oneliner level 1, but not supported for the metric child statement and its attribute *10*:

```
[edit protocols]
  isis {
    interface ge-0/0/0.0 {
      level 1 metric 10;
    }
  }
}
```

Options *comment-string*—Text of the comment. You must enclose it in quotation marks. In the comment string, you can include the comment delimiters `/* */` or `#`. If you do not specify any, the comment string is enclosed with the `/* */` comment delimiters. If a comment for the specified *statement* already exists, it is deleted and replaced with the new comment.

statement—Statement to which you are attaching the comment.

Required Privilege Level `configure`—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- [Adding Comments in a Junos OS Configuration on page 492](#)

commit

Syntax commit <<at <"string">> <and-quit> <check> <comment <"comment-string">>
 <confirmed> <display detail> <fast-synchronize> <minutes> <peers-synchronize >
 <synchronize <force> <scripts>>

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Option **fast-synchronize** added in Junos OS Release 12.2.
 Option **synchronize scripts** introduced in Junos OS Release 13.2.
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
 Option **peers-synchronize** introduced in Junos OS Release 14.2R6.

Description Commit the set of changes to the database and cause the changes to take operational effect.



NOTE: The **fast-synchronize** option is not supported in a QFX Series Virtual Chassis.



NOTE: Beginning in Junos OS 12.3, it is possible that FPCs brought offline using the **request chassis fpc slot fpc-slot offline** operational-mode CLI command can come online during a configuration commit or power-supply replacement procedure. As an alternative, use the **set fpc fpc-slot power off** configuration-mode command at the [edit chassis] hierarchy level to ensure that the FPCs remain offline.

Options **at <"string">**—(Optional) Save software configuration changes and activate the configuration at a future time, or upon reboot.

string is **reboot** or the future time to activate the configuration changes. Enclose the **string** value (including **reboot**) in quotation marks (" "). You can specify time in two formats:

- A time value in the form **hh:mm[:ss]** (hours, minutes, and optionally seconds)—Commit the configuration at the specified time, which must be in the future but before 11:59:59 PM on the day the **commit at** configuration command is issued. Use 24-hour time for the **hh** value; for example, **04:30:00** is 4:30:00 AM, and **20:00** is 8:00 PM. The time is interpreted with respect to the clock and time zone settings on the router.
- A date and time value in the form **yyyy-mm-dd hh:mm[:ss]** (year, month, date, hours, minutes, and, optionally, seconds)—Commit the configuration at the specified day and time, which must be after the **commit at** command is issued. Use 24-hour time for the **hh** value. For example, **2003-08-21 12:30:00** is 12:30 PM on August 21, 2003. The time is interpreted with respect to the clock and time zone settings on the router.

For example, **commit at "18:00:00"**. For date and time, include both values in the same set of quotation marks. For example, **commit at "2005-03-10 14:00:00"**.

A *commit check* is performed when you issue the **commit at** configuration mode command. If the result of the check is successful, then the current user is logged out of configuration mode, and the configuration data is left in a read-only state. No other commit can be performed until the scheduled commit is completed.



NOTE: If Junos OS fails before the configuration changes become active, all configuration changes are lost.

You cannot enter the **commit at** configuration command when there is a pending reboot.

You cannot enter the **request system reboot** command once you schedule a commit operation for a specific time in the future.

You cannot commit a configuration when a scheduled commit is pending. For information about how to use the **clear** command to cancel a scheduled configuration, see the [CLI Explorer](#).

and-quit—(Optional) Commit the configuration and, if the configuration contains no errors and the commit succeeds, exit from configuration mode.

check—(Optional) Verify the syntax of the configuration, but do not activate it.

comment <*comment-string*>—(Optional) Add a comment that describes the committed configuration. The comment can be as long as 512 bytes and must be typed on a single line. You cannot include a comment with the **commit check** command. Enclose *comment-string* in quotation marks (" "). For example, **commit comment "Includes changes recommended by SW Lab"**.

confirmed <*minutes*>—(Optional) Require that the commit be confirmed within the specified amount of time. To confirm a commit, enter either a **commit** or **commit check** command. If the commit is not confirmed within the time limit, the configuration rolls back automatically to the precommit configuration and a broadcast message is sent to

all logged-in users. To show when a rollback is scheduled, enter the **show system commit** command. The allowed range is 1 through 65,535 minutes, and the default is 10 minutes.

In Junos OS Release 11.4 and later, you can also use the **commit confirmed** command in the **[edit private]** configuration mode.

display detail—(Optional) Monitors the commit process.



NOTE: In Junos OS Release 10.4 and later, if the number of commit details or messages exceeds a page when used with the **| display detail** pipe option, the more pagination option on the screen is no longer available. Instead, the messages roll up on the screen by default, just like using the **commit** command with the **| no more** pipe option.

fast-synchronize—(Optional) Configure the commits to run in parallel on both the master and backup Routing Engines to reduce the time taken for commit synchronization.



NOTE: The **fast-synchronize** statement is not supported on QFX Series devices when used in a Virtual Chassis.

peers-synchronize—(Optional) Automatically synchronizes and commits MC-LAG configurations across the peers. The local peer (the requesting peer) on which you enable the **peers-synchronize** statement copies and loads its configuration to the remote (the responding) peer. Each peer then performs a syntax check on the configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both peers.

synchronize <force> <scripts>—(Optional) If your router has two Routing Engines, you can manually direct one Routing Engine to synchronize its configuration with the other by issuing the **commit synchronize** command. The Routing Engine on which you execute this command (the request Routing Engine) copies and loads its candidate configuration to the other Routing Engine (the responding Routing Engine). Both Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

It can happen that the **commit synchronize** command is initiated at the same time from both Routing Engines, which causes the process to hang. As of Junos OS Release 15.1, this is a temporary (20 seconds) anomaly, after which the user can try the **commit synchronize** command again.

The **commit synchronize** command does not work if the responding Routing Engine has uncommitted configuration changes. However, you can enforce commit synchronization on the Routing Engines by using the **force** option. When you issue the **commit synchronize** command with the **force** option from one Routing Engine, the configuration sessions on

the other Routing Engine are terminated and its configuration synchronized with that on the Routing Engine from which you issued the command.

When you issue the **commit synchronize** command with the **scripts** option, the device synchronizes all commit, event, lib, op, and SNMP scripts from the requesting Routing Engine to the responding Routing Engine and also commits and synchronizes the configuration. If the commit check operation fails for the requesting Routing Engine, the process stops, and the scripts are not copied to the responding Routing Engine. If the commit check or commit operation fails for the responding Routing Engine, the scripts are still synchronized, since the synchronization occurs prior to the commit check operation on the responding Routing Engine.

If the **load-scripts-from-flash** statement is configured for the requesting Routing Engine, the device synchronizes the scripts from flash memory on the requesting Routing Engine to flash memory on the responding Routing Engine. Otherwise, the device synchronizes the scripts from the hard disk on the requesting Routing Engine to the hard disk on the responding Routing Engine. The device synchronizes all scripts regardless of whether they are enabled in the configuration or have been updated since the last synchronization.



NOTE: When you issue the **commit synchronize** command, you must use the **apply-groups re0** and **re1** commands. For information about how to use groups, see [“Disabling Inheritance of a Junos OS Configuration Group” on page 620](#).

The responding Routing Engine must use Junos OS Release 5.0 or later.

Required Privilege Level

configure—To enter configuration mode.



NOTE: If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

```
load merge
load replace
load override
load update
```

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*

Related Documentation

- [Verifying a Junos OS Configuration on page 504, Committing a Junos OS Configuration on page 508](#)
- [Scheduling a Junos OS Commit Operation on page 513](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489](#)

- [Monitoring the Junos OS Commit Process on page 514](#)
- [Adding a Comment to Describe the Committed Configuration on page 515](#)
- [Committing Configurations on a Routing Matrix with a TX Matrix Plus Router](#)

Sample Output

commit | display detail

```

user@host> commit | display detail
-----
2011-08-24 01:08:08.00691 PDT: begin creating snapshots
2011-08-24 01:08:09.00210 PDT: end creating snapshots
2011-08-24 01:08:09.00211 PDT: begin preparing metadata
2011-08-24 01:08:09.00228 PDT: end preparing metadata
2011-08-24 01:08:09.00229 PDT: begin computing dcf root changes
2011-08-24 01:08:09.00236 PDT: end computing dcf root changes
2011-08-24 01:08:09.00244 PDT: begin computing additions
2011-08-24 01:08:09.00251 PDT: end computing additions
2011-08-24 01:08:09.00251 PDT: begin local object validation
2011-08-24 01:08:09.00251 PDT: end local object validation
2011-08-24 01:08:09.00252 PDT: begin update instances
2011-08-24 01:08:09.00252 PDT: end update instances
2011-08-24 01:08:09.00252 PDT: begin adjust metadata
2011-08-24 01:08:09.00252 PDT: end adjust metadata
2011-08-24 01:08:09.00253 PDT: begin validate metadata
2011-08-24 01:08:09.00253 PDT: end validate metadata
2011-08-24 01:08:09.00253 PDT: begin adjust allocations
2011-08-24 01:08:09.00254 PDT: end adjust allocations
2011-08-24 01:08:09.00254 PDT: begin adjust dependencies
2011-08-24 01:08:09.00254 PDT: end adjust dependencies
2011-08-24 01:08:09.00255 PDT: begin instance validation
2011-08-24 01:08:09.00255 PDT: end instance validation
2011-08-24 01:08:09.00255 PDT: begin opening all sessions eagerly
2011-08-24 01:08:09.00277 PDT: begin request #1 [login]
2011-08-24 01:08:09.00278 PDT: end request #1 [login]
2011-08-24 01:08:09.00325 PDT: begin processing globals
2011-08-24 01:08:09.00330 PDT: begin waiting for stamp check
(qfabric-default---node0)
2011-08-24 01:08:09.00334 PDT: end reply #1 [login]
2011-08-24 01:08:09.00351 PDT: end reply #1 [login]
2011-08-24 01:08:09.00451 PDT: begin request #2 [open]
2011-08-24 01:08:09.00451 PDT: end request #2 [open]
2011-08-24 01:08:09.00451 PDT: begin request #3 [get commit history]
2011-08-24 01:08:09.00452 PDT: end request #3 [get commit history]
2011-08-24 01:08:09.00452 PDT: begin request #4 [load]
2011-08-24 01:08:09.00453 PDT: end request #4 [load]
2011-08-24 01:08:09.00453 PDT: begin request #5 [load]
2011-08-24 01:08:09.00454 PDT: begin reply #2 [open]
2011-08-24 01:08:09.00456 PDT: end reply #2 [open]
2011-08-24 01:08:09.00457 PDT: begin reply #3 [get commit history]
2011-08-24 01:08:09.00475 PDT: end reply #3 [get commit history]
2011-08-24 01:08:09.00476 PDT: begin reply #4 [load]
2011-08-24 01:08:09.00499 PDT: begin reply #5 [load]
2011-08-24 01:08:09.00501 PDT: end waiting for stamp check
(qfabric-default---node0)
2011-08-24 01:08:09.00501 PDT: begin waiting for open (qfabric-default---node0)
2011-08-24 01:08:09.00502 PDT: end waiting for open (qfabric-default---node0)
2011-08-24 01:08:09.00504 PDT: end processing globals

```

```

2011-08-24 01:08:09.00617 PDT: end request #5 [load]
2011-08-24 01:08:09.00617 PDT: begin request #6 [check]
2011-08-24 01:08:09.00617 PDT: end request #6 [check]
2011-08-24 01:08:09.00619 PDT: end reply #5 [load]
2011-08-24 01:08:09.00619 PDT: begin reply #6 [check]
2011-08-24 01:08:09.00730 PDT: end session
2011-08-24 01:08:09.00752 PDT: end request #5 [load]
2011-08-24 01:08:09.00754 PDT: begin request #6 [check]
2011-08-24 01:08:09.00755 PDT: end request #6 [check]
2011-08-24 01:08:09.00881 PDT: end request #5 [load]
2011-08-24 01:08:09.00961 PDT: begin commit to devices
2011-08-24 01:08:10.00668 PDT: begin request #8 [get commit history]
2011-08-24 01:08:10.00669 PDT: end request #8 [get commit history]
2011-08-24 01:08:10.00721 PDT: end session
2011-08-24 01:08:10.00727 PDT: end commit to devices
2011-08-24 01:08:10.00733 PDT: begin committing metadata
2011-08-24 01:08:10.00772 PDT: end committing metadata
2011-08-24 01:08:10.00772 PDT: begin calling commit callbacks
2011-08-24 01:08:10.00773 PDT: end calling commit callbacks
commit complete

```

commit-interval (Batch Commits)

Syntax	<code>commit-interval <i>number-of-seconds-between-commits</i>;</code>
Hierarchy Level	[edit system commit server], [edit system commit synchronize server]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	For Junos OS batch commits, specify the time interval (in seconds) between two commit operations.
Options	<p><i>number-of-seconds-between-commits</i>—Time interval (in seconds) between two commit operations.</p> <p>Range: 1 through 30 seconds.</p> <p>Default: 5 seconds.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Batch Commit Server Properties on page 517

configuration-breadcrumbs

Syntax	configuration-breadcrumbs;
Hierarchy Level	[edit system login class]
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Enable the configuration breadcrumbs view in the CLI to display the location in the configuration hierarchy.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Enabling Configuration Breadcrumbs on page 654• <i>Defining Junos OS Login Classes</i>• <i>class</i>• <i>login</i>

copy

Syntax	<code>copy <i>existing-statement</i> to <i>new-statement</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Make a copy of an existing statement in the configuration.
Options	<i>existing-statement</i> —Statement to copy. <i>new-statement</i> —Copy of the statement.
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Copying a Junos OS Statement in the Configuration on page 473

days-to-keep-error-logs (Batch Commits)

Syntax	<code>days-to-keep-error-logs <i>days-to-keep-error-log-entries</i>;</code>
Hierarchy Level	[edit system commit server], [edit system commit synchronize server]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	For Junos OS batch commits, specify the number of days to keep the error logs.
Options	<i>days-to-keep-error-log-entries</i> —Number of days to keep the error logs. Range: 1 through 366 days Default: 1 day
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Batch Commit Server Properties on page 517

deactivate

Syntax	<code>deactivate (<i>statement</i> <i>identifier</i>)</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Add the inactive: tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the commit command.
Options	<p><i>identifier</i>—Identifier to which you are adding the inactive: tag. It must be an identifier at the current hierarchy level.</p> <p><i>statement</i>—Statement to which you are adding the inactive: tag. It must be a statement at the current hierarchy level.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• activate on page 660• delete on page 671• Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489.

delete

Syntax	<code>delete <statement-path> <identifier></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.</p> <p>Deleting a statement or an identifier effectively “unconfigures” or disables the functionality associated with that statement or identifier.</p> <p>If you do not specify <i>statement-path</i> or <i>identifier</i>, the entire hierarchy, starting at the current hierarchy level, is removed.</p>
Options	<p><i>statement-path</i>—(Optional) Path to an existing statement or identifier. Include this if the statement or identifier to be deleted is not at the current hierarchy level.</p> <p><i>identifier</i>—(Optional) Name of the statement or identifier to delete.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• deactivate on page 670• Deleting a Statement from a Junos OS Configuration on page 470

edit

Syntax	<code>edit <i>statement-path</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Move inside the specified statement hierarchy. If the statement does not exist, it is created.</p> <p>You cannot use the edit command to change the value of identifiers. You must use the set command.</p>
Options	<i>statement-path</i> —Path to the statement.
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• set on page 689• Displaying the Current Junos OS Configuration on page 497

exit

Syntax	exit <configuration-mode>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.
Options	<p>none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.</p> <p>configuration-mode—(Optional) Exit from configuration mode.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• top on page 700• up on page 703• Displaying the Current Junos OS Configuration on page 497

groups

```
Syntax  groups {
        group-name {
            configuration-data;
            when {
                chassis chassis-id;
                member member-id;
                model model-id;
                node node-id;
                peers [ names of peers ]
                routing-engine routing-engine-id;
                time <start-time> [to <end-time>];
            }
            conditional-data;
        }
        lccn-re0 {
            configuration-data;
        }
        lccn-re1 {
            configuration-data;
        }
    }
```

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Create a configuration group.

Options —

group-name—Name of the configuration group. To configure multiple groups, specify more than one **group-name**.

configuration-data—The configuration statements that are to be applied elsewhere in the configuration with the **apply-groups** statement, to have the target configuration inherit the statements in the group.

when conditional-data—Option introduced in Junos 11.3. The conditional statements that are to be applied when this configuration group is applied.

On routers that support multiple Routing Engines, you can also specify two special group names:

re0—Configuration statements that are to be applied to the Routing Engine in slot 0.

re1—Configuration statements that are to be applied to the Routing Engine in slot 1.

The configuration specified in group **re0** is applied only if the current Routing Engine is in slot 0; likewise, the configuration specified in group **re1** is applied only if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each

re0 or **re1** group contains at a minimum the configuration for the hostname and the management interface (**fxp0**). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

(Routing matrix only) The TX Matrix router supports group names for the Routing Engines in each connected T640 router in the following formats:



NOTE: The management Ethernet interface used for the TX Matrix Plus router, T1600 routers in a routing matrix, and PTX Series Packet Transport Routers, is **em0**. Junos OS automatically creates the router's management Ethernet interface, **em0**.

- **lccn-re0**—Configuration statements applied to the Routing Engine in slot 0 of the specified T640 router that is connected to a TX Matrix router.
 - **lccn-re1**—Configuration statements applied to the specified to the Routing Engine in slot 1 of the specified T640 router that is connected to a TX Matrix router.
- n* identifies the T640 router and can be from 0 through 3.

The remaining statements are explained separately.

Required Privilege Level configure—To enter configuration mode.

- Related Documentation**
- [Creating a Junos OS Configuration Group on page 615](#)
 - [apply-groups on page 658](#)
 - [apply-groups-except on page 659](#)

help

Syntax	<code>help <(apropos <i>string</i> reference <<i>statement-name</i>> syslog <<i>syslog-tag</i>> tip cli <i>number</i> topic <<i>word</i>>)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display help about available configuration statements or general information about getting help.
Options	<p>apropos <i>string</i>—(Optional) Display statement names and help text that matches the string specified. If the string contains spaces, enclose it in quotation marks (" "). You can also specify a regular expression for the string, using standard UNIX-style regular expression syntax.</p> <p>reference <<i>statement-name</i>>—(Optional) Display summary information for the statement. This information is based on summary descriptions that appear in the Junos configuration guides.</p> <p>syslog <<i>syslog-tag</i>>—(Optional) Display information about system log messages.</p> <p>tip cli <i>number</i>—(Optional) Display a tip about using the CLI. Specify the number of the tip you want to view.</p> <p>topic <<i>word</i>>—(Optional) Display usage guidelines for a topic or configuration statement. This information is based on subjects that appear in the Junos configuration guides.</p> <p>Entering the help command without an option provides introductory information about how to use the help command.</p>
Required Privilege Level	configure—To enter configuration mode.
Related Documentation	<ul style="list-style-type: none">• Getting Online Help from the Junos OS Command-Line Interface on page 447

insert

Syntax	insert < <i>statement-path</i> > <i>identifier1</i> (before after) <i>identifier2</i>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Insert an identifier in to an existing hierarchy.
Options	<p>after—Place <i>identifier1</i> after <i>identifier2</i>.</p> <p>before—Place <i>identifier1</i> before <i>identifier2</i>.</p> <p><i>identifier1</i>—Existing identifier.</p> <p><i>identifier2</i>—New identifier to insert.</p> <p><i>statement-path</i>—(Optional) Path to the existing identifier.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Inserting a New Identifier in a Junos OS Configuration on page 481

load

Syntax	load (factory-default merge override patch replace set update) load (<i>filename</i> terminal) <relative>
QFX Series	load (dhcp-snooping <i>filename</i>)
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Load a configuration from an ASCII configuration file, from terminal input, or from the factory default. Your current location in the configuration hierarchy is ignored when the load operation occurs.



NOTE: **load** can be run from configuration mode only.

Options **dhcp-snooping**—(QFX Series switches) Loads DHCP snooping entries.

factory-default—Loads the factory configuration. The factory configuration contains the manufacturer's suggested configuration settings. The factory configuration is the router or switch's first configuration and is loaded when the router or switch is first installed and powered on.



NOTE: To load the factory default configuration, you must first **unprotect** any protected hierarchies in the configuration.

filename—Name of the file to load. For information about specifying the filename, see [“Specifying Filenames and URLs” on page 576](#).

merge—Combine the configuration that is currently shown in the CLI with the configuration.

override—Discard the entire configuration that is currently shown in the CLI and load the entire configuration. Marks every object as changed.

patch—Change part of the configuration and mark only those parts as changed.

replace—Look for a **replace** tag in *filename*, delete the existing statement of the same name, and replace it with the configuration.

set—Merge a set of commands with an existing configuration. This option executes the configuration instructions line by line as they are stored in a file or from a terminal. The instructions can contain any configuration mode command, such as **set**, **edit**, **exit**, and **top**.

relative—(Optional) Execute set of commands until the current edit point.

terminal—Use the text you type at the terminal as input to the configuration. Type Ctrl+d to end terminal input.

update—Discard the entire configuration that is currently shown in the CLI, and load the entire configuration. Marks changed objects only.



NOTE: If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

```
load merge
load replace
load override
load update
```

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

Required Privilege Level configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- [Loading a Configuration from a File on page 544](#)

maximum-aggregate-pool (Batch Commits)

Syntax	<code>maximum-aggregate-pool <i>maximum-number-of-commits-to-aggregate</i>;</code>
Hierarchy Level	[edit system commit server], [edit system commit synchronize server]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	For Junos OS batch commits, specify the maximum number of individual commit operations that are aggregated or merged into a single commit operation.
Options	<p><i>maximum-number-of-commits-to-aggregate</i>—Maximum number of individual commit operations that are aggregated or merged into a single commit operation.</p> <p>Range: 1 through 4294967295</p> <p>Default: 5</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Batch Commit Server Properties on page 517

maximum-entries (Batch Commits)

Syntax	<code>maximum-entries <i>number-of-entries</i>;</code>
Hierarchy Level	[edit system commit server], [edit system commit synchronize server]
Release Information	Statement introduced in Junos OS Release 12.1.
Description	For Junos OS batch commits, specify the maximum number of commit jobs that are included in the commit queue.
Options	<i>number-of-entries</i> —Maximum number of commit jobs that are included in the commit queue.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Batch Commit Server Properties on page 517

protect

Syntax	<code>protect (hierarchy statement identifier)</code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Protect a hierarchy, statement, or identifier from modification or deletion.
Options	none
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Example: Protecting the Junos OS Configuration from Modification or Deletion on page 551

quit

Syntax	quit <configuration-mode>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms.
Options	<p>none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.</p> <p>configuration-mode—(Optional) Exit from configuration mode.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• top on page 700• up on page 703• Displaying the Current Junos OS Configuration on page 497

rename

Syntax `rename <statement-path> identifier1 to identifier2`

Release Information Command introduced before Junos OS Release 7.4.

Description Rename an existing configuration statement or identifier.

Options *identifier1*—Existing identifier to rename.

identifier2—New name of identifier.

statement-path—(Optional) Path to an existing statement or identifier.



NOTE: For example, to rename interface `ge-0/0/0.0` to `ge-0/0/10.0` at the following hierarchy level:

```
logical-systems {
  logical-system-abc {
    (...)
    protocols {
      ospf {
        area 0.0.0.0 {
          interface ge-0/1/0.0;
```

Issue the following command:

```
rename logical-systems logical-system-abc protocols ospf area 0.0.0.0 interface
ge-0/1/0.0.0 to interface ge-0/1/10.0
```

Required Privilege Level `configure`—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- [Renaming an Identifier in a Junos OS Configuration on page 476](#)

replace

Syntax	replace pattern <i>pattern1</i> with <i>pattern2</i> <upto <i>n</i> >
Release Information	Command introduced in Junos OS Release 7.6.
Description	Replace identifiers or values in a configuration. For more information, refer to KB30332 .
Options	<p><i>pattern1</i>—Text string or regular expression that defines the identifiers or values you want to match.</p> <p><i>pattern2</i>—Text string or regular expression that replaces the identifiers and values located with <i>pattern1</i>.</p> <p>Juniper Networks uses standard UNIX-style regular expression syntax (as defined in POSIX 1003.2). If the regular expression contains spaces, operators, or wildcard characters, enclose the expression in quotation marks. Greedy qualifiers (match as much as possible) are supported. Lazy qualifiers (match as little as possible) are not.</p> <p>upto <i>n</i>—Number of objects replaced. The value of <i>n</i> controls the total number of objects that are replaced in the configuration (not the total number of times the pattern occurs). Objects at the same hierarchy level (siblings) are replaced first. Multiple occurrences of a pattern within a given object are considered a single replacement. If you do not specify an upto option, all identifiers and values in the configuration that match <i>pattern1</i> are replaced.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Using Global Replace in a Junos OS Configuration on page 603

rollback

Syntax	<code>rollback <number rescue></code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	<p>Return to a previously committed configuration. The software saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command.</p> <p>The currently operational Junos OS configuration is stored in the file juniper.conf, and the last three committed configurations are stored in the files juniper.conf.1, juniper.conf.2, and juniper.conf.3. These four files are located in the directory /config, which is on the router's flash drive. The remaining 46 previous committed configurations, the files juniper.conf.4 through juniper.conf.49, are stored in the directory /var/db/config, which is on the router's hard disk.</p> <p>During rollback, the configuration you specify is loaded from the associated file. Only objects in the rollback configuration that differ from the previously loaded configuration are marked as changed (equivalent to load update).</p>
Options	<p>none (Optional)—Return to the most recently saved configuration.</p> <p>number—(Optional) Configuration to return to. The range of values is from 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49. The default is 0.</p> <p>rescue—(Optional) Return to the rescue configuration.</p>
Required Privilege Level	rollback—To roll back to configurations other than the one most recently committed.
Related Documentation	<ul style="list-style-type: none"> • Returning to a Previously Committed Junos OS Configuration on page 535 • Creating and Returning to a Rescue Configuration on page 538

run

Syntax	<code>run <i>command</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Run a top-level CLI command without exiting from configuration mode.
Options	<i>command</i> —CLI top-level command.
Required Privilege Level	configure—To enter configuration mode.
Related Documentation	<ul style="list-style-type: none">• Understanding Junos OS CLI Configuration Mode on page 456

save

Syntax	<code>save <i>filename</i></code>
QFX Series	<code>save (dhcp-snooping <i>filename</i>)</code>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Save the configuration to an ASCII file. The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy.</p> <p>When saving a file to a remote system, the software uses the scp/ssh protocol.</p>
Options	<p><i>filename</i>—Name of the saved file. You can specify a filename in one of the following ways:</p> <ul style="list-style-type: none"> • <i>filename</i>—File in the user's home directory (the current directory) on the local flash drive. • <i>path/filename</i>—File on the local flash drive. • <i>/var/filename</i> or <i>/var/path/filename</i>—File on the local hard disk. • <i>a:filename</i> or <i>a:path/filename</i>—File on the local drive. The default path is / (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format. • <i>hostname:/path/filename</i>, <i>hostname:filename</i>, <i>hostname:path/filename</i>, or <i>scp://hostname/path/filename</i>—File on an scp/ssh client. This form is not available in the worldwide version of Junos OS. The default path is the user's home directory on the remote system. You can also specify <i>hostname</i> as <i>username@hostname</i>. • <i>ftp://hostname/path/filename</i>—File on an FTP server. You can also specify <i>hostname</i> as <i>username @hostname</i> or <i>username:password @hostname</i>. The default path is the user's home directory. To specify an absolute path, the path must start with the string %2F; for example, <i>ftp://hostname/%2Fpath/filename</i>. To have the system prompt you for the password, specify <i>prompt</i> in place of the password. If a password is required, and you do not specify the password or <i>prompt</i>, an error message is displayed: <pre> user@host> file copy ftp://username@ftp.hostname.net//filename file copy ftp.hostname.net: Not logged in. user@host> file copy ftp://username:prompt@ftphostname.net//filename </pre> <p>Password for <i>username@ftp.hostname.net</i>:</p> • <i>http://hostname/path/filename</i>—File on a Hypertext Transfer Protocol (HTTP) server. You can also specify <i>hostname</i> as <i>username@hostname</i> or <i>username:password@hostname</i>. If a password is required and you omit it, you are prompted for it. • <i>re0:/path/filename</i> or <i>re1:/path/filename</i>—File on a local Routing Engine.

Required Privilege Level configure—To enter configuration mode.

Related Documentation

- [Deactivating and Reactivating Statements and Identifiers in a Junos OS Configuration on page 489](#)

server (Batch Commits)

Syntax

```
server {  
    commit-interval <number-of-seconds-between-commits>;  
    days-to-keep-error-logs <days-to-keep-error-log-entries>;  
    maximum-aggregate-pool <maximum-number-of-commits-to-aggregate>;  
    maximum-entries <number-of-entries>;  
    traceoptions {  
        file filename;  
        files number;  
        flag (all | batch | commit-server | configuration);  
        size maximum-file-size;  
        (world-readable | no-world-readable);  
    }  
}
```

Hierarchy Level [edit system commit]

Release Information Statement introduced in Junos OS Release 12.1.

Description Configure the system commit to occur in batches. Configure parameters for aggregating and saving batch commits.

Options [commit-interval](#)—Configure the interval between commits.

[days-to-keep-error-logs](#)—Configure the number of days to keep log entries.

[maximum-aggregate-pool](#)—Configure the maximum number of commits to aggregate together.

[maximum-entries](#) —Configure the maximum number of commit entries.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring Batch Commit Server Properties on page 517](#)

set

Syntax	<code>set <<i>statement-path</i>> <i>identifier</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change.
Options	<p><i>identifier</i>—Name of the statement or identifier to set.</p> <p><i>statement-path</i>—(Optional) Path to an existing statement hierarchy level. If that hierarchy level does not exist, it is created.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• edit on page 672• Displaying the Current Junos OS Configuration on page 497

show

Syntax	<code>show <statement-path> <identifier></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the current configuration.
Options	<p><code>none</code>—Display the entire configuration at the current hierarchy level.</p> <p><code>identifier</code>—(Optional) Display the configuration for the specified identifier.</p> <p><code>statement-path</code>—(Optional) Display the configuration for the specified statement hierarchy path.</p>
Required Privilege Level	<code>configure</code> —To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• show display inheritance on page 694• show display omit on page 695• show display set on page 696• show display set relative on page 697• show groups junos-defaults on page 698• Displaying the Current Junos OS Configuration on page 497

show configuration

Syntax	<code>show configuration</code> <code><statement-path></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display the configuration that currently is running on the router or switch, which is the last committed configuration.
Options	<p>none—Display the entire configuration.</p> <p>statement-path—(Optional) Display one of the following hierarchies in a configuration. (Each statement-path option has additional suboptions not described here. See the appropriate feature guide or EX Series switch documentation for more information.)</p> <ul style="list-style-type: none"> • access—Network access configuration. • access-profile—Access profile configuration. • accounting-options—Accounting data configuration. • applications—Applications defined by protocol characteristics. • apply-groups—Groups from which configuration data is inherited. • chassis—Chassis configuration. • chassis network-services—Current running mode. • class-of-service—Class-of-service configuration. • diameter—Diameter base protocol layer configuration. • ethernet-switching-options—(EX Series switch only) Ethernet switching configuration. • event-options—Event processing configuration. • firewall—Firewall configuration. • forwarding-options—Options that control packet sampling. • groups—Configuration groups. • interfaces—Interface configuration. • jsrc—JSRC partition configuration. • jsrc-partition—JSRC partition configuration. • logical-systems—Logical system configuration. • poe—(EX Series switch only) Power over Ethernet configuration. • policy-options—Routing policy option configuration. • protocols—Routing protocol configuration.

- **routing-instances**—Routing instance configuration.
- **routing-options**—Protocol-independent routing option configuration.
- **security**—Security configuration.
- **services**—Service PIC applications configuration.
- **snmp**—Simple Network Management Protocol configuration.
- **system**—System parameters configuration.
- **virtual-chassis**—(EX Series switch only) Virtual Chassis configuration.
- **vlan**—(EX Series switch only) VLAN configuration.

Additional Information The portions of the configuration that you can view depend on the user class that you belong to and the corresponding permissions. If you do not have permission to view a portion of the configuration, the text **ACCESS-DENIED** is substituted for that portion of the configuration. If you do not have permission to view authentication keys and passwords in the configuration, because the **secret** permission bit is not set for your user account, the text **SECRET-DATA** is substituted for that portion of the configuration. If an identifier in the configuration contains a space, the identifier is displayed in quotation marks.

Likewise, when you issue the **show configuration** command with the **| display set** pipe option to view the configuration as **set** commands, those portions of the configuration that you do not have permissions to view are substituted with the text **ACCESS-DENIED**.

Required Privilege Level view

Related Documentation

- [Displaying the Current Junos OS Configuration on page 497](#)
- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)

List of Sample Output [show configuration on page 692](#)
[show configuration policy-options on page 693](#)

Output Fields This command displays information about the current running configuration.

Sample Output

show configuration

```
user@host> show configuration
## Last commit: 2006-10-31 14:13:00 PST by user1 version "8.2I0 [userc]"; ## last
changed: 2006-10-31 14:05:53 PST
system {
    host-name exhost;
    domain-name ex1.net;
    backup-router 198.51.100.254;
    time-zone America/Los_Angeles;
    default-address-selection;
    name-server {
        192.0.2.254;
        192.0.2.249;
```

```

        192.0.2.176;
    }
    services {
        telnet;
    }
    tacplus-server {
        10.2.3.4 {
            secret /* SECRET-DATA */;
            ...
        }
    }
}
interfaces {
    ...
}
protocols {
    isis {
        export "direct routes";
    }
}
policy-options {
    policy-statement "direct routes" {
        from protocol direct;
        then accept;
    }
}

```

show configuration policy-options

```

user@host> show configuration policy-options
policy-options {
    policy-statement "direct routes" {
        from protocol direct;
        then accept;
    }
}

```

show | display inheritance

Syntax show | display inheritance <brief | defaults | no-comments | terse>

Release Information Command introduced before Junos OS Release 7.4.

Description Show the inherited configuration data and information about the source group from which the configuration has been inherited. Show interface ranges configuration data in expanded format and information about the source interface-range from which the configuration has been expanded

```
user@host# show system ports | display inheritance defaults
## 'console' was inherited from group 'junos-defaults'
## 'vt100' was inherited from group 'junos-defaults'
## console type vt100;
```

```
user@host# show system login class readonly | display inheritance
## 'interface' was inherited from group global'
## 'network' was inherited from group global'
## 'routing' was inherited from group global'
## 'system' was inherited from group global'
## 'trace' was inherited from group global'
## 'view' was inherited from group global'
##
permissions [ interface network routing system trace view ];
```

```
user@host# show system login class readonly | display inheritance no-comments
permissions [ interface network routing system trace view ];
```

- Options**
- **brief**—Display brief output for the command.
 - **defaults**—Display the Junos OS defaults that have been applied to the configuration.
 - **no-comments**—Display configuration information without inline comments marked with ##.
 - **terse**—Display terse output with inheritance details as inline comment.

Required Privilege Level view

Related Documentation

- [Using Junos OS Defaults Groups on page 640](#)

show | display omit

Syntax show | display omit

Release Information Command introduced in Junos OS Release 8.2.

Description Display configuration statements (including those marked as hidden by the **apply-flags omit** configuration statement).

```
user@host# show | display omit
system {
  apply-flags omit;
  login {
    message lengthy-login-message;
  }
}
```

Required Privilege Level view

Related Documentation • [show on page 690](#)

show | display set

Syntax	show display set
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Display the configuration as a series of configuration mode commands required to recreate the configuration from the top level of the hierarchy as set commands</p> <pre>user@host# show display set set interfaces fe-0/0/0 unit 0 family inet address 192.168.1.230/24 set interfaces fe-0/0/0 unit 0 family iso set interfaces fe-0/0/0 unit 0 family mpls set interfaces fe-0/0/0 unit 1 family inet address 10.0.0.1/8 deactivate interfaces fe-0/0/0 unit 1</pre>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show on page 690• Displaying set Commands from the Junos OS Configuration on page 501

show | display set relative

Syntax	show display set relative
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Display the configuration as a series of configuration mode commands required to re-create the configuration from the current hierarchy level.</p> <pre>[edit interfaces fe-0/0/0] user@host# show unit 0 { family inet { address 192.107.1.230/24; } family iso; family mpls; } inactive: unit 1 { family inet { address 10.0.0.1/8; } } user@host# show display set relative set unit 0 family inet address 192.107.1.230/24 set unit 0 family iso set unit 0 family mpls set unit 1 family inet address 10.0.0.1/8 deactivate unit 1</pre>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Displaying set Commands from the Junos OS Configuration on page 501

show groups junos-defaults

Syntax show groups junos-defaults

Release Information Command introduced before Junos OS Release 7.4.

Description Display the full set of available preset statements from the Junos OS defaults group.

```
user@host# show groups junos-defaults
groups {
  junos-defaults {
    applications {
      # File Transfer Protocol
      application junos-ftp {
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
      }
      # Trivial File Transfer Protocol
      application junos-tftp {
        application-protocol tftp;
        protocol udp;
        destination-port 69;
      }
      # RPC port mapper on TCP
      application junos-rpc-portmap-tcp {
        application-protocol rpc-portmap;
        protocol tcp;
        destination-port 111;
      }
      # RPC port mapper on UDP
    }
  }
}
```

Required Privilege Level view

Related Documentation • [Using Junos OS Defaults Groups on page 640](#)

status

Syntax	status
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the users currently editing the configuration.
Required Privilege Level	configure—To enter configuration mode. <ul style="list-style-type: none">• “Displaying Users Currently Editing the Junos OS Configuration” on page 504.

top

Syntax	<code>top <configuration-command></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Return to the top level of configuration command mode, which is indicated by the [edit] banner.
Options	<i>configuration-command</i> —(Optional) Issue configuration mode commands from the top of the hierarchy.
Required Privilege Level	configure—To enter configuration mode.
Related Documentation	<ul style="list-style-type: none">• Displaying the Current Junos OS Configuration on page 497• exit on page 673• up on page 703

tracoptions (Batch Commits)

Syntax	<pre>tracoptions { file <i>filename</i>; files <i>number</i>; flag (all batch commit-server configuration); size <i>maximum-file-size</i>; (world-readable no-world-readable); }</pre>
Hierarchy Level	<pre>[edit system commit server], [edit system commit synchronize server]</pre>
Release Information	Statement introduced in Junos OS Release 12.1.
Description	For Junos OS batch commits, configure tracing operations.
Options	file <i>name</i> —Name of the file to receive the output of the tracing operation.



NOTE: If you configure **tracoptions** and do not explicitly specify a **filename** for logging the events, the batch commit events are logged in the **commitd** file (**var/log/commitd**) by default.

files *number*—Maximum number of trace files.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—All tracing operations flags.
- **batch**—Tracing operations for batch events.
- **commit-server**—Tracing operations for commit server events.
- **configuration**—Tracing operations for the reading of configuration.

size—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

world-readable | no-world-readable—**readable**—Grant all users permission to read archived log files, or restrict the permission only to the root user and users who have the Junos OS maintenance permission.

Required Privilege Level	<pre>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</pre>
---------------------------------	---

Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Batch Commit Server Properties on page 517
------------------------------	---

unprotect

Syntax	<code>unprotect (<i>hierarchy</i> <i>statement</i> <i>identifier</i>)</code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Unprotect a protected hierarchy, configuration statement, or an identifier.
Options	none
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• top on page 700• up on page 703• Displaying the Current Junos OS Configuration on page 497

up

Syntax	<code>up <number> <configuration-command></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Move up one level in the statement hierarchy.
Options	<p>none—Move up one level in the configuration hierarchy.</p> <p><i>configuration-command</i>—(Optional) Issue configuration mode commands from a location higher in the hierarchy.</p> <p><i>number</i>—(Optional) Move up the specified number of levels in the configuration hierarchy.</p>
Required Privilege Level	configure—To enter configuration mode.
Related Documentation	<ul style="list-style-type: none">• Displaying the Current Junos OS Configuration on page 497• exit on page 673• top on page 700

update

Syntax update

Release Information Command introduced in Junos OS Release 7.5.

Description Update private candidate configuration with a copy of the most recently committed configuration, including your private changes.



NOTE: The **update** command is available only when you are in configure private mode.

Required Privilege Level configure—To enter configuration mode.

Related Documentation

- [Updating the configure private Configuration on page 496.](#)

when

Syntax	<pre> when { chassis <i>chassis-id</i>; member <i>member-id</i>; model <i>model-id</i>; node [<i>names of peers</i>]<i>node-id</i>; peers [<i>names of peers</i>]; routing-engine <i>routing-engine-id</i>; time <<i>start-time</i>> [to <<i>end-time</i>>]; } </pre>
Hierarchy Level	[edit groups <i>group-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 11.3.</p> <p>peers option added in Junos OS Release 14.2R6 for the MX Series.</p> <p>peers option added in Junos OS Release 15.1X53-D60 for the QFX Series.</p>
Description	<p>Define conditions under which the configuration group should be applied. Conditions include the type of chassis, model, or Routing Engine, virtual chassis member, cluster node, and start and optional end time of day. If you specify multiple conditions in a single configuration group, all conditions must be met before the configuration group is applied.</p>
Options	<p>chassis <i>chassis-id</i>—Specify the chassis type of the router. Valid types include SCC0, SCC1, LCC0, LCC1 ... LCC3.</p> <p>member <i>member-id</i>—Specify the name of the member of the virtual chassis.</p> <p>model <i>model-id</i>—Specify the model name of the router, such as m7i or tx100.</p> <p>node <i>node-id</i>—Specify the cluster node.</p> <p>peers [<i>names of peers</i>]—Specify the names of the MC-LAG peers participating in commit synchronization.</p> <p>routing-engine <i>routing-engine-id</i>—Specify the type of Routing Engine, re0 or re1.</p> <p>time <<i>start-time</i>> [to <<i>end-time</i>>]—Specify the start time or time duration for this configuration group to be applied. If only the start time is specified, the configuration group is applied at the specified time and remains in effect until the time is changed. If the end time is specified, then on each day, the applied configuration group is started and stopped at the specified times. The syntax for specifying the time is: time <<i>start-time</i>> [to <<i>end-time</i>>] using the time format yyyy-mm-dd.hh:mm, hh:mm, or hh.</p>
Required Privilege Level	configure—To enter configuration mode.
Related Documentation	<ul style="list-style-type: none"> • Creating a Junos OS Configuration Group on page 615 • apply-groups on page 658

- [apply-groups-except on page 659](#)
- [groups on page 674](#)

wildcard delete

Syntax	<code>wildcard delete <statement-path> <identifier> <regular-expression></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.</p> <p>Deleting a statement or an identifier effectively “unconfigures” or disables the functionality associated with that statement or identifier.</p> <p>If you do not specify <i>statement-path</i> or <i>identifier</i>, the entire hierarchy starting at the current hierarchy level is removed.</p>
Options	<p><i>identifier</i>—(Optional) Name of the statement or identifier to delete.</p> <p><i>regular-expression</i>—(Optional) The pattern based on which you want to delete multiple items. When you use the wildcard command to delete related configuration items, the <i>regular-expression</i> must be the final statement.</p> <p><i>statement-path</i>—(Optional) Path to an existing statement or identifier. Include this if the statement or identifier to be deleted is not at the current hierarchy level.</p>
Required Privilege Level	configure—To enter configuration mode. Other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• Example: Using Global Replace in a Junos OS Configuration—Using the upto Option on page 608.

CHAPTER 31

Junos OS CLI Environment Commands

- `set cli complete-on-space`
- `set cli directory`
- `set cli idle-timeout`
- `set cli prompt`
- `set cli restart-on-upgrade`
- `set cli screen-length`
- `set cli screen-width`
- `set cli terminal`
- `set cli timestamp`
- `set date`
- `show cli`
- `show cli`
- `show cli authorization`
- `show cli directory`
- `show cli history`

set cli complete-on-space

Syntax	set cli complete-on-space (off on)
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set the command-line interface (CLI) to complete a partial command entry when you type a space or a tab. This is the default behavior of the CLI.
Options	off —Turn off command completion. on —Allow either a space or a tab to be used for command completion.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>CLI User Interface Overview</i>• show cli on page 720
List of Sample Output	set cli complete-on-space on page 710
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli complete-on-space

In the following example, pressing the Spacebar changes the partial command entry from **com** to **complete-on-space**. The example shows how adding the keyword **off** at the end of the command disables command completion.

```
user@host> set cli com<Space>
user@host>set cli complete-on-space off
Disabling complete-on-space
```

set cli directory

Syntax	set cli directory <i>directory</i>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set the current working directory.
Options	<i>directory</i> —Pathname of the working directory.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>CLI User Interface Overview</i>• <i>show cli directory</i>
List of Sample Output	set cli directory on page 711
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli directory

```
user@host> set cli directory /var/tmp
Current directory: /var/tmp
```

set cli idle-timeout

Syntax	set cli idle-timeout < <i>minutes</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set the maximum time that an individual session can be idle before the user is logged off the router or switch.
Options	<i>minutes</i> —(Optional) Maximum idle time. The range of values, in minutes, is 0 through 100,000. If you do not issue this command, and the user's login class does not specify this value, the user is never forced off the system after extended idle times. Setting the value to 0 disables the timeout.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>CLI User Interface Overview</i>• show cli on page 720
List of Sample Output	set cli idle-timeout on page 712
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli idle-timeout

```
user@host> set cli idle-timeout 60
Idle timeout set to 60 minutes
```


set cli prompt

Syntax	set cli prompt <i>string</i>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set the prompt so that it is displayed within the CLI.
Options	<i>string</i> —CLI prompt string. To include spaces in the prompt, enclose the string in quotation marks. By default, the string is <i>username@hostname</i> .
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>CLI User Interface Overview</i>• show cli on page 720
List of Sample Output	set cli prompt on page 713
Output Fields	When you enter this command, the new CLI prompt is displayed.

Sample Output

set cli prompt

```
user@host> set cli prompt lab1-router>
lab1-router>
```

set cli restart-on-upgrade

Syntax	set cli restart-on-upgrade string (off on)
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	For an individual session, set the CLI to prompt you to restart the router or switch after upgrading the software.
Options	off —Disables the prompt. on —Enables the prompt.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>CLI User Interface Overview</i>• show cli on page 720
List of Sample Output	set cli restart-on-upgrade on page 714
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli restart-on-upgrade

```
user@host> set cli restart-on-upgrade on
Enabling restart-on-upgrade
```

set cli screen-length

Syntax	set cli screen-length <i>length</i>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Set terminal screen length.</p> <pre>user@host> set cli screen-length 75 Screen Length set to 75</pre>
Options	<p><i>length</i>—Number of lines of text that the terminal screen displays. The range of values, in number of lines, is 24 through 100,000. The default is 24.</p> <p>The point at which the ---(more)--- prompt appears on the screen is a function of this setting and the settings for the set cli screen-width and set cli terminal commands.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Setting the Screen Length on page 647• Setting the Junos OS CLI Screen Length and Width on page 647• set cli screen-width on page 716• set cli terminal on page 717• show cli on page 722

set cli screen-width

Syntax `set cli screen-width <width>`

Release Information Command introduced before Junos OS Release 7.4.

Description Set the terminal screen width.

```
user@host> set cli screen-width 132
Screen width set to 132
```

Options *width*—Number of characters in a line. The value is **0** or in the range of **40** through **1024**. The default value is **80**.



NOTE: In Junos OS Release 13.2 and earlier, the value of *width* is in the range of **0** through **1024**.

Required Privilege Level view


Related Documentation

- [Setting the Screen Width on page 648](#)
- [set cli screen-length on page 715](#)
- [set cli terminal on page 717](#)
- [show cli on page 722](#)

set cli terminal

Syntax	set cli terminal <i>terminal-type</i>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Set the terminal type.</p> <pre>user@host> set cli terminal xterm</pre>
Options	<p><i>terminal-type</i>—Type of terminal that is connected to the Ethernet management port:</p> <ul style="list-style-type: none">• ansi—ANSI-compatible terminal (80 characters by 24 lines)• small-xterm—Small xterm window (80 characters by 24 lines)• vt100—VT100-compatible terminal (80 characters by 24 lines)• xterm—Large xterm window (80 characters by 65 lines)
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Setting the Terminal Type on page 646

set cli timestamp

Syntax	set cli timestamp (format <i>timestamp-format</i> disable)
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Set a timestamp for CLI output.
Options	<p>format <i>timestamp-format</i>—Set the date and time format for the timestamp. The timestamp format you specify can include the following placeholders in any order:</p> <ul style="list-style-type: none"> • %m—Two-digit month • %d—Two-digit date • %T—Six-digit hour, minute, and seconds <p>disable—Remove the timestamp from the CLI.</p>
<div>  <p>NOTE: A timestamp is displayed by default when no command output is generated.</p> </div>	
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • CLI User Interface Overview • show cli on page 720
List of Sample Output	set cli timestamp on page 718
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli timestamp

```
user@host> set cli timestamp format '%m-%d-%T'
'04-21-17:39:13'
CLI timestamp set to: '%m-%d-%T'
```

set date

Syntax	set date (<i>date-time</i> ntp < <i>ntp-server</i> > <source-address <i>source-address</i> >)
Release Information	Command introduced before Junos OS Release 7.4.
Description	Set the date and time. user@host> set date ntp 21 Apr 17:22:02 ntpdate[3867]: step time server 172.17.27.46 offset 8.759252 sec
Options	<ul style="list-style-type: none"> • <i>date-time</i>—Specify date and time in one of the following formats: <ul style="list-style-type: none"> • <i>YYYYMMDDHHMM.SS</i> • “<i>month DD, YYYY HH:MM(am pm)</i>” • <i>ntp</i>—Configure the router to synchronize the current date and time setting with a Network Time Protocol (NTP) server. • <i>ntp-server</i>—(Optional) Specify the IP address of one or more NTP servers. • <i>source-address source-address</i>—(Optional) Specify the source address that is used by the router to contact the remote NTP server.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Setting the Date and Time Locally</i>

show cli

List of Syntax	Syntax on page 720 Syntax (QFX Series and OCX Series) on page 720
Syntax	show cli
Syntax (QFX Series and OCX Series)	show cli <authorization> <directory> <history <i>count</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display configured CLI settings.
Options	This command has no options.
Required Privilege Level	view
List of Sample Output	show cli on page 721
Output Fields	Table 69 lists the output fields for the show cli command. Output fields are listed in the approximate order in which they appear.

Table 69: show cli Output Fields

Field Name	Field Description
CLI complete-on-space	Capability to complete a partial command entry when you type a space or a tab: on or off .
CLI idle-timeout	Maximum time that an individual session can be idle before the user is logged out from the router or switch. When this feature is enabled, the number of minutes is displayed. Otherwise, the state is disabled .
CLI restart-on-upgrade	CLI is set to prompt you to restart the router or switch after upgrading the software: on or off .
CLI screen-length	Number of lines of text that the terminal screen displays.
CLI screen-width	Number of characters in a line on the terminal screen.
CLI terminal	Terminal type.
CLI is operating in	Mode: enhanced .
CLI timestamp	Date and time format for the timestamp. If the timestamp is not set, the state is disabled .
CLI working directory	Pathname of the working directory.

Sample Output

show cli

```
user@host> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen-length set to 47
CLI screen-width set to 132
CLI terminal is 'vt100'
CLI is operating in enhanced mode
CLI timestamp disabled
CLI working directory is '/var/tmp'
```

show cli

Syntax	show cli
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Display configured CLI settings.</p> <pre>user@host> show cli CLI complete-on-space set to on CLI idle-timeout disabled CLI restart-on-upgrade set to on CLI screen-length set to 47 CLI screen-width set to 132 CLI terminal is 'vt100' CLI is operating in enhanced mode CLI timestamp disabled CLI working directory is '/var/tmp'</pre>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show cli authorization on page 723• show cli directory on page 724

show cli authorization

Syntax show cli authorization

Release Information Command introduced before Junos OS Release 7.4.

Description Display the permissions for the current user.

```
user@host> show cli authorization
Current user: 'root' login: 'boojum' class '(root)'
Permissions:
Permissions:
  admin      -- Can view user accounts
  admin-control-- Can modify user accounts
  clear      -- Can clear learned network info
  configure  -- Can enter configuration mode
  control    -- Can modify any config
  edit       -- Can edit full files
  field      -- Can use field debug commands
  floppy     -- Can read and write the floppy
  interface  -- Can view interface configuration
  interface-control-- Can modify interface configuration
  network    -- Can access the network
  reset      -- Can reset/restart interfaces and daemons
  routing    -- Can view routing configuration
  routing-control-- Can modify routing configuration
  shell      -- Can start a local shell
  snmp       -- Can view SNMP configuration
  snmp-control-- Can modify SNMP configuration
  system     -- Can view system configuration
  system-control-- Can modify system configuration
  trace      -- Can view trace file settings
  trace-control-- Can modify trace file settings
  view       -- Can view current values and statistics
  maintenance -- Can become the super-user
  firewall   -- Can view firewall configuration
  firewall-control-- Can modify firewall configuration
  secret     -- Can view secret statements
  secret-control-- Can modify secret statements
  rollback   -- Can rollback to previous configurations
  security   -- Can view security configuration
  security-control-- Can modify security configuration
  access     -- Can view access configuration
  access-control-- Can modify access configuration
  view-configuration-- Can view all configuration (not including secrets)
  flow-tap   -- Can view flow-tap configuration
  flow-tap-control-- Can modify flow-tap configuration
  idp-profiler-operation-- Can Profiler data
  pgcp-session-mirroring-- Can view pgcp session mirroring configuration
  pgcp-session-mirroring-control-- Can modify pgcp session mirroring configuration
  storage    -- Can view fibre channel storage protocol configuration
  storage-control-- Can modify fibre channel storage protocol configuration
  all-control -- Can modify any configuration
```

Required Privilege Level view

show cli directory

Syntax	show cli directory
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the current working directory. user@host> show cli directory Current directory: /var/tmp
Required Privilege Level	view

show cli history

Syntax	show cli history < <i>count</i> >
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Display a list of previous CLI commands.</p> <pre>user@host> show cli history 11:14:14 -- show arp 11:22:10 -- show cli authorization 11:27:12 -- show cli history</pre>
Options	<p>none—Display all previous CLI commands.</p> <p><i>count</i>—(Optional) Maximum number of commands to display.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Displaying the Junos OS CLI Command and Word History on page 454

CHAPTER 32

Junos OS CLI Operational Mode Commands

- `configure`
- `file`
- `help`
- `|` (pipe)
- `request`
- `request system commit server pause`
- `request system commit server queue cleanup`
- `request system commit server start`
- `restart`
- `set`
- `show system commit server queue`
- `show system commit server status`

configure

Syntax	configure <batch> <dynamic> <exclusive> <private>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enter configuration mode. When this command is entered without any optional keywords, everyone can make configuration changes and commit all changes made to the configuration.
Options	<p>none—Enter configuration mode.</p> <p>batch—(Optional) Work in the batch commit mode where commit operations are executed in batches.</p> <p>dynamic—(Optional) Configure routing policies and certain routing policy objects in a dynamic database that is not subject to the same verification required in the standard configuration database. As a result, the time it takes to commit changes to the dynamic database is much shorter than for the standard configuration database. You can then reference these policies and policy objects in routing policies you configure in the standard database.</p> <p>exclusive—(Optional) Lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. Other users can enter and exit configuration mode, but they cannot change the configuration.</p> <p>private—(Optional) Allow multiple users to edit different parts of the configuration at the same time and to commit only their own changes, or to roll back without interfering with one another's changes. You cannot commit changes in configure private mode when another user is in configure exclusive mode.</p>
Additional Information	For more information about the different methods of entering configuration mode and the restrictions that apply, see the <i>Junos OS Administration Library for Routing Devices</i> .
Required Privilege Level	configure
Related Documentation	<ul style="list-style-type: none"> • show configuration on page 691
List of Sample Output	configure on page 729
Output Fields	When you enter this command, you are placed in configuration mode and the system prompt changes from <i>hostname></i> to <i>hostname#</i> .

Sample Output

configure

```
user@host> configure
Entering configuration mode
[edit]
user@host#
```

file

Syntax	file <archive checksum compare copy delete list rename show source address>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Archive files from the device, copy files to and from the router or switch, calculate the file checksum, compare files, delete a file from the device, list files on the device, rename a file, show file contents, or show the local address to initiate a connection.
Options	<p>archive (Optional)—Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.</p> <p>checksum (Optional)—Calculate the Message Digest 5 (MD5) checksum of a file.</p> <p>compare (Optional)—Compare two local files and describe the differences between them in default, context, or unified output styles.</p> <p>copy (Optional)—Copy files from one place to another on the local switch or between the local switch and a remote system.</p> <p>delete (Optional)—Delete a file on the local switch.</p> <p>list (Optional)—Display a list of files on the local switch.</p> <p>rename (Optional)—Rename a file on the local switch.</p> <p>show (Optional)—Display the contents of a file.</p> <p>source address (Optional)—Specify the source address of the local file.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• Viewing Files and Directories on a Device Running Junos OS on page 573

help

Syntax	<code>help < (apropos <i>string</i> reference <<i>statement-name</i>> syslog <<i>syslog-tag</i>> tip cli <i>number</i> topic <<i>word</i>>)></code>
Release Information	Command introduced before Junos OS Release 7.4. apropos option added in Junos OS Release 8.0.
Description	Display help about available operational commands, configuration statements, or general information about getting help. Entering the help command without an option provides introductory information about how to use the help and ? commands.
Options	<p>apropos <i>string</i>—(Optional) Display command names and help text that matches the string specified. If the string contains spaces, enclose it in quotation marks (" "). You can also specify a regular expression for the string, using standard UNIX-style regular expression syntax.</p> <p>reference <<i>statement-name</i>>—(Optional) Display summary information for a configuration statement. This information is based on summary descriptions that appear in the Junos configuration guides.</p> <p>syslog <<i>syslog-tag</i>>—(Optional) Display information about system log messages.</p> <p>tip cli <i>number</i>—(Optional) Display a tip about using the CLI. Specify the number of the tip you want to view.</p> <p>topic <<i>word</i>>—(Optional) Display usage guidelines for a topic or configuration statement. This information is based on subjects that appear in the Junos configuration guides.</p>
Required Privilege Level	None
Related Documentation	<ul style="list-style-type: none"> • Getting Online Help from the Junos OS Command-Line Interface on page 447

| (pipe)

Syntax	(compare count display (changed commit-scripts detail set inheritance json omit xml) except <i>pattern</i> find <i>pattern</i> hold last <i>lines</i> match <i>pattern</i> no-more refresh <i>interval</i> request message (all <i>account@terminal</i>) resolve <full-names> save <i>filename</i> append <i>filename</i> tee trim <i>columns</i>)
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>display commit-scripts option added in Junos OS Release 7.4.</p> <p>tee option added in Junos OS Release 14.1.</p> <p>display json option added in Junos OS Release 14.2.</p> <p>compare display xml option added in Junos OS Release 15.1.</p>
Description	Filter the output of an operational mode or a configuration mode command.
Options	<p>append <i>filename</i>—Append the output to a file.</p> <p>compare (<i>filename</i> rollback <i>n</i>)—Compare configuration changes with another configuration file. In operational mode, use the show configuration command. In configuration mode, use the show command. See “Comparing Configurations and Displaying the Differences in Text” on page 590</p> <p>compare display xml—Compare configuration changes with the active configuration and display them in XML format. In operational mode, use the show configuration command. In configuration mode, use the show command. See “Understanding the show compare display xml Command Output” on page 528.</p> <p>count—Display the number of lines in the output.</p> <p>display—Display additional information about the configuration contents.</p> <p>changed—Tag changes with junos:changed attribute (XML only).</p> <p>commit-scripts—(Configuration mode only) Display all statements that are in a configuration, including statements that were generated by transient changes. For more information, see the <i>Automation Scripting Feature Guide</i>.</p> <p>detail—(Configuration mode only) Display configuration data detail.</p> <p>inheritance <brief default no-comments groups terse>—(Configuration mode only) Display inherited configuration data and source group.</p> <p>json—Display the output for operational commands and configuration data in JavaScript Object Notation (JSON) format.</p> <p>omit—(Configuration mode only) Display configuration statements omitted by the apply-flags omit configuration statement.</p> <p>set—Display the configuration as a series of configuration mode commands required to re-create the configuration.</p>

xml—(Operational mode only) Display the command output as Junos XML protocol (Extensible Markup Language [XML]) tags.

except *pattern*—Ignore text matching a regular expression when searching the output. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks.

find *pattern*—Display the output starting at the first occurrence of text matching a regular expression. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks (" ").

hold—Hold text without exiting the **--More--** prompt.

last *lines*—Display the last number of lines you want to view from the end of the configuration. However, when the number of lines requested is less than the number of lines that the screen length setting permits you to display, Junos returns as many lines as permitted by the screen length setting. For more information on using the **last *lines*** option, see [“Displaying Output Beginning with the Last Entries” on page 594](#).

match *pattern*—Search for text matching a regular expression. If the regular expression contains spaces, operators, or wildcard characters, enclose it in quotation marks.

no-more—Display output all at once rather than one screen at a time.

resolve—(Operational mode only) Convert IP addresses into Domain Name System (DNS) names. Truncates to fit original size unless **full-names** is specified. To prevent the names from being truncated, use the **full-names** option.

refresh *interval*—Refresh the display of the command according to the interval specified. The screen gets refreshed periodically to show you the current output of the command until you quit the command. The default refresh interval is one second. However, you can also explicitly specify a value from 1 through 604800 for the refresh interval.

request message (all | *account@terminal*)—Display command output on the terminal of a specific user logged in to your router, or on the terminals of all users logged in to your router.

save *filename*—Save the output to a file or URL. For information about specifying the filename, see [“Specifying Filenames and URLs” on page 576](#).

tee—Allows you to both display the command output on screen and write it to a file. Unlike the UNIX **tee** command, if the file cannot be opened, just an error message is displayed.

trim *columns*—Trim specified number of columns from the start line. Only positive values are accepted. An error message appears if a negative value is given.

Required Privilege Level view

**Related
Documentation**

- [Displaying the Current Junos OS Configuration on page 497.](#)
- [Using the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 587](#)
- [Using Regular Expressions with the Pipe \(| \) Symbol to Filter Junos OS Command Output on page 588](#)
- [Pipe \(| \) Filter Functions in the Junos OS Command-Line Interface on page 590](#)

request

Syntax request <chassis | ipsec switch | message | mpls | routing-engine | security | services | system | flow-collector | support information>

Release Information Command introduced before Junos OS Release 7.4.

Description Stop or reboot router components, switch between primary and backup components, display messages, and display system information.



CAUTION: Halt the backup Routing Engine before you remove it or shut off the power to the router; otherwise, you might need to reinstall the Junos OS.



NOTE: If your router contains two Routing Engines and you want to shut the power off to the router or remove a Routing Engine, you must first halt the backup Routing Engine (if it has been upgraded) and then the master Routing Engine. To halt a Routing Engine, enter the `request system halt` command. You can also halt both Routing Engines at the same time by issuing the `request system halt both-routing-engines` command.

If you want to reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) and then the master Routing Engine.



NOTE: If you reboot the TX Matrix router, all the T640 master Routing Engines connected to the TX Matrix router reboot. If you halt both Routing Engines on a TX Matrix router, all the T640 Routing Engines connected to the TX Matrix router are also halted. Likewise, if you reboot the TX Matrix Plus router, all the T1600 or T4000 master Routing Engines connected to the TX Matrix Plus router reboot. If you halt both Routing Engines on a TX Matrix Plus router, all the T1600 or T4000 Routing Engines connected to the TX Matrix Plus router are also halted.



NOTE: If you insert a Flexible PIC Concentrator (FPC) into your router, you may need to issue the `request chassis fpc` command (or press the online button) to bring the FPC online. This applies to FPCs in M20, M40, M40e, M160, M320, and T Series routers. For command usage, see the `request chassis fpc` command description in the [CLI Explorer](#).

Additional Information Most **request** commands are described in the *Junos System Basics and Services Command Reference*. The following **request** commands are described in the *Junos Interfaces Command Reference*: **request ipsec switch** and **request services**.

Required Privilege Level maintenance

Related Documentation

- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)

request system commit server pause

Syntax `request system commit server pause`

Release Information Command introduced in Junos OS Release 12.1.

Description Pause the commit server.



NOTE: If you issue this command when a commit job is in process, the batch commit server pauses only after the current commit job is completed.

Options This command has no options.

Required Privilege Level view

Related Documentation • [Example: Configuring Batch Commit Server Properties on page 517](#)

Sample Output

When you enter the `request system commit server pause` command, you are provided feedback on the status of your request.

`request system commit server pause`

```
user@host> request system commit server pause
```

```
Successfully paused the commit server.
```

request system commit server queue cleanup

Syntax	request system commit server queue cleanup <id <i>commit-id</i>> <job-status (error pending success)>
Release Information	Command introduced in Junos OS Release 12.1.
Description	Clean up the batch commit queue.
Options	id <i>commit-id</i> —(Optional) Clean up batch commit operation status messages for a specific commit ID. job-status —(Optional) Clean up batch commit operation status messages for the following: <ul style="list-style-type: none">• error—Clean up status messages for batch commit operations that have errors.• pending—Clean up status messages for batch commit operations that are pending.• success—Clean up status messages for batch commit operations that are successful.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Batch Commit Server Properties on page 517
List of Sample Output	request system commit server queue cleanup id on page 738 request system commit server queue cleanup job-status success on page 738

Sample Output

When you enter the **request system commit server queue cleanup** command, you are provided feedback on the status of your request.

[request system commit server queue cleanup id](#)

```
user@host> request system commit server queue cleanup id 1008  
  
Successfully cleaned up jobs.
```

[request system commit server queue cleanup job-status success](#)

```
user@host> request system commit server queue cleanup job-status success  
  
Successfully cleaned up jobs.
```

request system commit server start

Syntax	<code>request system commit server start</code>
Release Information	Command introduced in Junos OS Release 12.1.
Description	Start the commit server.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Batch Commit Server Properties on page 517

Sample Output

When you enter the `request system commit server start` command, you are provided feedback on the status of your request.

request system commit server start

```
user@host> request system commit server start
```

```
Successfully started the commit server.
```

restart

List of Syntax [Syntax on page 740](#)

[Syntax \(ACX Series Routers\) on page 740](#)
[Syntax \(EX Series Switches\) on page 740](#)
[Syntax \(MX Series Routers\) on page 741](#)
[Syntax \(QFX Series\) on page 741](#)
[Syntax \(Routing Matrix\) on page 741](#)
[Syntax \(TX Matrix Routers\) on page 741](#)
[Syntax \(TX Matrix Plus Routers\) on page 742](#)
[Syntax \(MX Series Routers\) on page 742](#)
[Syntax \(QFX Series\) on page 742](#)

Syntax restart

```

<adaptive-services | ancpd-service | application-identification | audit-process |
  auto-configuration | captive-portal-content-delivery | ce-l2tp-service | chassis-control |
  class-of-service | clksyncd-service | database-replication | datapath-trace-service
  | dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture |
  ecc-error-logging | ethernet-connectivity-fault-management
  | ethernet-link-fault-management | event-processing | firewall
  | general-authentication-service | gracefully | iccp-service | idp-policy | immediately
  | interface-control | ipsec-key-management | kernel-replication | l2-learning | l2cpd-service
  | l2tp-service | l2tp-universal-edge | lacp | license-service | link-management
  | local-policy-decision-function | mac-validation | mib-process | mounstd-service
  | mpls-traceroute | mspd | multicast-snooping | named-service | nfsd-service |
  packet-triggered-subscribers | peer-selection-service | pgm | pic-services-logging | pki-service
  | ppp | ppp-service | pppoe | protected-system-domain-service |
  redundancy-interface-process | remote-operations | root-system-domain-service | routing
  <logical-system logical-system-name> | sampling | sbc-configuration-process | sdk-service
  | service-deployment | services | snmp | soft | static-subscribers | statistics-service |
  subscriber-management | subscriber-management-helper | tunnel-oamd | usb-control |
  vrrp | web-management>
<gracefully | immediately | soft>

```

Syntax (ACX Series Routers)

```

restart
<adaptive-services | audit-process | auto-configuration | autoinstallation | chassis-control |
  class-of-service | clksyncd-service | database-replication | dhcp-service | diameter-service
  | disk-monitoring | dynamic-flow-capture | ethernet-connectivity-fault-management
  | ethernet-link-fault-management | event-processing | firewall
  | general-authentication-service | gracefully | immediately | interface-control |
  ipsec-key-management | l2-learning | lacp | link-management | mib-process | mounstd-service
  | mpls-traceroute | mspd | named-service | nfsd-service | pgm | pki-service | ppp | pppoe |
  redundancy-interface-process | remote-operations | routing | sampling | sdk-service
  | secure-neighbor-discovery | service-deployment | services | snmp | soft | statistics-service |
  subscriber-management | subscriber-management-helper | tunnel-oamd | vrrp>

```

Syntax (EX Series Switches)

```

restart
<autoinstallation | chassis-control | class-of-service | database-replication | dhcp |
  dhcp-service | diameter-service | dot1x-protocol | ethernet-link-fault-management |
  ethernet-switching | event-processing | firewall | general-authentication-service |
  interface-control | kernel-replication | l2-learning | lacp | license-service | link-management
  | lldpd-service | mib-process | mounstd-service | multicast-snooping | pgm |

```

redundancy-interface-process | remote-operations | routing | secure-neighbor-discovery
| service-deployment | sflow-service | snmp | vrrp | web-management>

Syntax (MX Series Routers) restart
<adaptive-services | ancpd-service | application-identification | audit-process |
auto-configuration | captive-portal-content-delivery | ce-l2tp-service | chassis-control |
class-of-service | clksyncd-service | database-replication | datapath-trace-service
| dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture |
ecc-error-logging | ethernet-connectivity-fault-management
| ethernet-link-fault-management | event-processing | firewall |
general-authentication-service | gracefully | iccp-service | idp-policy | immediately
| interface-control | ipsec-key-management | kernel-replication | l2-learning | l2cpd-service
| l2tp-service | l2tp-universal-edge | lacp | license-service | link-management
| local-policy-decision-function | mac-validation | mib-process | mountd-service
| mpls-traceroute | mspd | multicast-snooping | named-service | nfsd-service |
packet-triggered-subscribers | peer-selection-service | pgm | pic-services-logging |
pki-service | ppp | ppp-service | pppoe | protected-system-domain-service |
redundancy-interface-process | remote-operations | root-system-domain-service | routing
| routing <logical-system *logical-system-name*> | sampling | sbc-configuration-process |
sdk-service | service-deployment | services | snmp | soft | static-subscribers | statistics-service |
subscriber-management | subscriber-management-helper | tunnel-oamd | usb-control |
vrrp | web-management>
<all-members>
<gracefully | immediately | soft>
<local>
<member *member-id*>

Syntax (QFX Series) restart
<adaptive-services | audit-process | chassis-control | class-of-service | dialer-services |
diameter-service | dlsw | ethernet-connectivity | event-processing | fibre-channel | firewall
| general-authentication-service | igmp-host-services | interface-control |
ipsec-key-management | isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process |
named-service | network-access-service | nstrace-process | pgm | ppp | pppoe |
redundancy-interface-process | remote-operations | *logical-system-name*> | routing |
sampling | secure-neighbor-discovery | service-deployment | snmp | usb-control |
web-management>
<gracefully | immediately | soft>

Syntax (Routing Matrix) restart
<adaptive-services | audit-process | chassis-control | class-of-service | disk-monitoring |
dynamic-flow-capture | ecc-error-logging | event-processing | firewall | interface-control
| ipsec-key-management | kernel-replication | l2-learning | l2tp-service | lacp |
link-management | mib-process | pgm | pic-services-logging | ppp | pppoe |
redundancy-interface-process | remote-operations | routing <logical-system
logical-system-name> | sampling | service-deployment | snmp>
<all | all-lcc | lcc *number*>
<gracefully | immediately | soft>

Syntax (TX Matrix Routers) restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp-service |
diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging |
event-processing | firewall | interface-control | ipsec-key-management | kernel-replication
| l2-learning | l2tp-service | lacp | link-management | mib-process | pgm | pic-services-logging
| ppp | pppoe | redundancy-interface-process | remote-operations | routing <logical-system
logical-system-name> | sampling | service-deployment | snmp | statistics-service>

	<p><all-chassis all-lcc lcc <i>number</i> scc></p> <p><gracefully immediately soft></p>
Syntax (TX Matrix Plus Routers)	<p>restart</p> <p><adaptive-services audit-process chassis-control class-of-service dhcp-service diameter-service disk-monitoring dynamic-flow-capture ecc-error-logging event-processing firewall interface-control ipsec-key-management kernel-replication l2-learning l2tp-service lacp link-management mib-process pgm pic-services-logging ppp pppoe redundancy-interface-process remote-operations routing <logical-system <i>logical-system-name</i>> sampling service-deployment snmp statistics-service></p> <p><all-chassis all-lcc all-sfc lcc <i>number</i> sfc <i>number</i>></p> <p><gracefully immediately soft></p>
Syntax (MX Series Routers)	<p>restart</p> <p><adaptive-services ancpd-service application-identification audit-process auto-configuration captive-portal-content-delivery ce-l2tp-service chassis-control class-of-service clksyncd-service database-replication datapath-trace-service dhcp-service diameter-service disk-monitoring dynamic-flow-capture ecc-error-logging ethernet-connectivity-fault-management ethernet-link-fault-management event-processing firewall general-authentication-service gracefully iccp-service idp-policy immediately interface-control ipsec-key-management kernel-replication l2-learning l2cpd-service l2tp-service l2tp-universal-edge lacp license-service link-management local-policy-decision-function mac-validation mib-process mobile-ip mountd-service mpls-traceroute mspd multicast-snooping named-service nfsd-service packet-triggered-subscribers peer-selection-service pgcp-service pgm pic-services-logging pki-service ppp ppp-service pppoe protected-system-domain-service redundancy-interface-process remote-operations root-system-domain-service routing routing <logical-system <i>logical-system-name</i>> sampling sbc-configuration-process sdk-service service-deployment services services pgcp gateway <i>gateway-name</i> snmp soft static-subscribers statistics-service subscriber-management subscriber-management-helper tunnel-oamd usb-control vrrp web-management></p> <p><all-members></p> <p><gracefully immediately soft></p> <p><local></p> <p><member <i>member-id</i>></p>
Syntax (QFX Series)	<p>restart</p> <p><adaptive-services audit-process chassis-control class-of-service dialer-services diameter-service dlsr ethernet-connectivity event-processing fibre-channel firewall general-authentication-service igmp-host-services interface-control ipsec-key-management isdn-signaling l2ald l2-learning l2tp-service mib-process named-service network-access-service nstrace-process pgm ppp pppoe redundancy-interface-process remote-operations <i>logical-system-name</i>> routing sampling secure-neighbor-discovery service-deployment snmp usb-control web-management></p> <p><gracefully immediately soft></p>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 12.2 for ACX Series routers.</p>

Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Options added:

- **dynamic-flow-capture** in Junos OS Release 7.4.
- **dls** in Junos OS Release 7.5.
- **event-processing** in Junos OS Release 7.5.
- **ppp** in Junos OS Release 7.5.
- **l2ald** in Junos OS Release 8.0.
- **link-management** in Release 8.0.
- **pgcp-service** in Junos OS Release 8.4.
- **sbc-configuration-process** in Junos OS Release 9.5.
- **services pgcp gateway** in Junos OS Release 9.6.
- **sfc** and **all-sfc** for the TX Matrix Router in Junos OS Release 9.6.

Description Restart a Junos OS process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router or switch to drop calls and interrupt transmission, resulting in possible loss of data.

Options **none**—Same as **gracefully**.

adaptive-services—(Optional) Restart the configuration management process that manages the configuration for stateful firewall, Network Address Translation (NAT), intrusion detection services (IDS), and IP Security (IPsec) services on the Adaptive Services PIC.

all-chassis—(TX Matrix and TX Matrix Plus routers only) (Optional) Restart the software process on all chassis.

all-lcc—(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process on all T640 routers connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process on all T1600 routers connected to the TX Matrix Plus router.

all-members—(MX Series routers only) (Optional) Restart the software process for all members of the Virtual Chassis configuration.

all-sfc—(TX Matrix Plus routers only) (Optional) For a TX Matrix Plus router, restart the software processes for the TX Matrix Plus router (or switch-fabric chassis).

ancpd-service—(Optional) Restart the Access Node Control Protocol (ANCP) process, which works with a special Internet Group Management Protocol (IGMP) session to collect outgoing interface mapping events in a scalable manner.

application-identification—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.

audit-process—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, analyzing, and tracking usage patterns, for billing a user based on the amount of time or type of services accessed.

auto-configuration—(Optional) Restart the Interface Auto-Configuration process.

autoinstallation—(EX Series switches only) (Optional) Restart the autoinstallation process.

captive-portal-content-delivery—(Optional) Restart the HTTP redirect service by specifying the location to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.

ce-l2tp-service—(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Universal Edge Layer 2 Tunneling Protocol (L2TP) process, which establishes L2TP tunnels and Point-to-Point Protocol (PPP) sessions through L2TP tunnels.

chassis-control—(Optional) Restart the chassis management process.

class-of-service—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.

clksyncd-service—(Optional) Restart the external clock synchronization process, which uses synchronous Ethernet (SyncE).

database-replication—(EX Series switches and MX Series routers only) (Optional) Restart the database replication process.

datapath-trace-service—(Optional) Restart the packet path tracing process.

dhcp—(EX Series switches only) (Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.

dhcp-service—(Optional) Restart the Dynamic Host Configuration Protocol process.

dialer-services—(EX Series switches only) (Optional) Restart the ISDN dial-out process.

diameter-service—(Optional) Restart the diameter process.

disk-monitoring—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.

dls—(QFX Series only) (Optional) Restart the data link switching (DLSw) service.

dot1x-protocol—(EX Series switches only) (Optional) Restart the port-based network access control process.

dynamic-flow-capture—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on Monitoring Services III PICs.

ecc-error-logging—(Optional) Restart the error checking and correction (ECC) process, which logs ECC parity errors in memory on the Routing Engine.

ethernet-connectivity-fault-management—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

ethernet-link-fault-management—(EX Series switches and MX Series routers only)
(Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.

ethernet-switching—(EX Series switches only) (Optional) Restart the Ethernet switching process.

event-processing—(Optional) Restart the event process (eventd).

fibre-channel—(QFX Series only) (Optional) Restart the Fibre Channel process.

firewall—(Optional) Restart the firewall management process, which manages the firewall configuration and enables accepting or rejecting packets that are transiting an interface on a router or switch.

general-authentication-service—(EX Series switches and MX Series routers only)
(Optional) Restart the general authentication process.

gracefully—(Optional) Restart the software process.

iccp-service—(Optional) Restart the Inter-Chassis Communication Protocol (ICCP) process.

idp-policy—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.

immediately—(Optional) Immediately restart the software process.

interface-control—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.

ipsec-key-management—(Optional) Restart the IPsec key management process.

isdn-signaling—(QFX Series only) (Optional) Restart the ISDN signaling process, which initiates ISDN connections.

kernel-replication—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.

l2-learning—(Optional) Restart the Layer 2 address flooding and learning process.

l2cpd-service—(Optional) Restart the Layer 2 Control Protocol process, which enables features such as Layer 2 protocol tunneling and nonstop bridging.

l2tp-service— (M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Layer 2 Tunneling Protocol (L2TP) process, which sets up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiating Multilink PPP if it is implemented.

l2tp-universal-edge— (MX Series routers only) (Optional) Restart the L2TP process, which establishes L2TP tunnels and PPP sessions through L2TP tunnels.

lACP— (Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG, and to enable the transmission and reception processes for the link to function in an orderly manner.

lcc number— (TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process for a specific T640 router that is connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

license-service— (EX Series switches only) (Optional) Restart the feature license management process.

link-management— (TX Matrix and TX Matrix Plus routers and EX Series switches only) (Optional) Restart the Link Management Protocol (LMP) process, which establishes and maintains LMP control channels.

lldpd-service— (EX Series switches only) (Optional) Restart the Link Layer Discovery Protocol (LLDP) process.

local— (MX Series routers only) (Optional) Restart the software process for the local Virtual Chassis member.

local-policy-decision-function— (Optional) Restart the process for the Local Policy Decision Function, which regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

mac-validation— (Optional) Restart the Media Access Control (MAC) validation process, which configures MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX Series routers.

member *member-id*— (MX Series routers only) (Optional) Restart the software process for a specific member of the Virtual Chassis configuration. Replace ***member-id*** with a value of 0 or 1.

mib-process— (Optional) Restart the Management Information Base (MIB) version II process, which provides the router's MIB II agent.

mobile-ip— (Optional) Restart the Mobile IP process, which configures Junos OS Mobile IP features.

moundd-service— (EX Series switches and MX Series routers only) (Optional) Restart the service for NFS mount requests.

mpls-traceroute— (Optional) Restart the MPLS Periodic Traceroute process.

mspd— (Optional) Restart the Multiservice process.

multicast-snooping— (EX Series switches and MX Series routers only) (Optional) Restart the multicast snooping process, which makes Layer 2 devices, such as VLAN switches, aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.

named-service— (Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.

network-access-service— (QFX Series only) (Optional) Restart the network access process, which provides the router's Challenge Handshake Authentication Protocol (CHAP) authentication service.

nfsd-service— (Optional) Restart the Remote NFS Server process, which provides remote file access for applications that need NFS-based transport.

packet-triggered-subscribers— (Optional) Restart the packet-triggered subscribers and policy control (PTSP) process, which allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device.

peer-selection-service— (Optional) Restart the Peer Selection Service process.

pgcp-service— (Optional) Restart the pgcpd service process running on the Routing Engine. This option does not restart pgcpd processes running on mobile station PICs. To restart pgcpd processes running on mobile station PICs, use the **services pgcp gateway** option.

pgm— (Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.

pic-services-logging— (Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.

pki-service—(Optional) Restart the PKI Service process.

ppp—(Optional) Restart the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.

ppp-service—(Optional) Restart the Universal edge PPP process, which is the encapsulation protocol process for transporting IP traffic across universal edge routers.

pppoe—(Optional) Restart the Point-to-Point Protocol over Ethernet (PPPoE) process, which combines PPP that typically runs over broadband connections with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator.

protected-system-domain-service—(Optional) Restart the Protected System Domain (PSD) process.

redundancy-interface-process—(Optional) Restart the ASP redundancy process.

remote-operations—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.

root-system-domain-service—(Optional) Restart the Root System Domain (RSD) service.

routing—(ACX Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the routing protocol process.

routing <logical-system *logical-system-name*>—(Optional) Restart the routing protocol process, which controls the routing protocols that run on the router or switch and maintains the routing tables. Optionally, restart the routing protocol process for the specified logical system only.

sampling—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.

sbc-configuration-process—(Optional) Restart the session border controller (SBC) process of the border signaling gateway (BSG).

scc—(TX Matrix routers only) (Optional) Restart the software process on the TX Matrix router (or switch-card chassis).

sdk-service—(Optional) Restart the SDK Service process, which runs on the Routing Engine and is responsible for communications between the SDK application and Junos OS. Although the SDK Service process is present on the router, it is turned off by default.

secure-neighbor-discovery—(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.

sfc *number*—(TX Matrix Plus routers only) (Optional) Restart the software process on the TX Matrix Plus router (or switch-fabric chassis). Replace *number* with 0.

service-deployment—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.

services—(Optional) Restart a service.

services pgcp gateway gateway-name—(Optional) Restart the pgcpd process for a specific border gateway function (BGF) running on an MS-PIC. This option does not restart the pgcpd process running on the Routing Engine. To restart the pgcpd process on the Routing Engine, use the **pgcp-service** option.

sflow-service—(EX Series switches only) (Optional) Restart the flow sampling (sFlow technology) process.

snmp—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.

soft—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.

static-subscribers—(Optional) Restart the static subscribers process, which associates subscribers with statically configured interfaces and provides dynamic service activation and activation for these subscribers.

statistics-service—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.

subscriber-management—(Optional) Restart the Subscriber Management process.

subscriber-management-helper—(Optional) Restart the Subscriber Management Helper process.

tunnel-oamd—(Optional) Restart the Tunnel OAM process, which enables the Operations, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.

usb-control—(MX Series routers) (Optional) Restart the USB control process.

vrrp—(ACX Series routers, EX Series switches, and MX Series routers only) (Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.

web-management—(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the Web management process.

Required Privilege Level reset

**Related
Documentation**

- [Overview of Junos OS CLI Operational Mode Commands on page 563](#)

List of Sample Output [restart interfaces on page 750](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

set

Syntax	<code>set <statement-path> identifier</code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change.
Options	<p><i>identifier</i>—Name of the statement or identifier to set.</p> <p><i>statement-path</i>—(Optional) Path to an existing statement hierarchy level. If that hierarchy level does not exist, it is created.</p>
Required Privilege Level	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
Related Documentation	<ul style="list-style-type: none">• edit on page 672• Displaying the Current Junos OS Configuration on page 497

show system commit server queue

Syntax `show system commit server queue`
`<id commit-id>`
`<job-status (all| error| pending| success)>`
`<patch (none | id commit-id) | (job-status (all | error | pending | success))>`

Release Information Command introduced in Junos OS Release 12.1.

Description Display the status of commit server queue transactions.



NOTE: Only 50 successful commit jobs are stored in the database and displayed in the output. When the fifty-first job is committed, the first job is deleted from the database and is no longer displayed in the output.

Options `id commit-id`—(Optional) Display the batch commit operation status messages for a specific commit ID.

`job-status`—(Optional) Display batch commit operation status messages for the following batch commit statuses:

- `all`—Status messages for all batch commit operations.
- `error`—Status messages for batch commit operations that have errors.
- `pending`—Status messages for batch commit operations that are pending.
- `success`—Status messages for batch commit operations that are successful.

`patch (none | id commit-id) | job-status (all | error | pending | success)`—(Optional) Display the patch file containing the configuration changes for all batch commit operations, a specific batch commit ID, or a specific job status.

Required Privilege Level view

Related Documentation [• Example: Configuring Batch Commit Server Properties on page 517](#)

List of Sample Output [show system commit server queue on page 752](#)
[show system commit server queue job-status success on page 753](#)
[show system commit server queue patch on page 753](#)

Sample Output

show system commit server queue

```
user@host> show system commit server queue
```

```
Pending commits:
none
```


Completed commits:

Id: 1000

Last Modified: Tue Nov 1 22:46:43 2011

Status: Successfully committed 1000

Id: 1002

Last Modified: Tue Nov 1 22:50:35 2011

Status: Successfully committed 1002

Id: 1004

Last Modified: Tue Nov 1 22:51:48 2011

Status: Successfully committed 1004

Id: 1007

Last Modified: Wed Nov 2 01:08:04 2011

Status: Successfully committed 1007

Id: 1009

Last Modified: Wed Nov 2 01:16:45 2011

Status: Successfully committed 1009

Id: 1010

Last Modified: Wed Nov 2 01:19:25 2011

Status: Successfully committed 1010

Id: 1011

Last Modified: Wed Nov 2 01:28:16 2011

Status: Successfully committed 1011

Error commits:

Id: 1008

Last Modified: Wed Nov 2 01:08:18 2011

Status: Error while committing 1008

show system commit server queue job-status success

user@host> show system commit server queue job-status success

Completed commits:

Id: 1000

Last Modified: Tue Nov 1 22:46:43 2011

Status: Successfully committed 1000

Id: 1001

Last Modified: Tue Nov 1 22:47:02 2011

Status: Successfully committed 1001

show system commit server queue patch

user@host> show system commit server queue patch

Pending commits:

none

Completed commits:

Id: 1000

Last Modified: Tue Nov 1 22:46:43 2011

Status: Successfully committed 1000

Patch:

[edit system commit]

```
+ server {
+   days-to-keep-error-logs 4294967295;
+   traceoptions {
+       file commitd_nov;
+       flag all;
+   }
+ }
Id: 1002
Last Modified: Tue Nov  1 22:50:35 2011
Status: Successfully committed 1002
```

Patch:

```
[edit system commit server]
- days-to-keep-error-logs 4294967295;
  Id: 1004
  Last Modified: Tue Nov  1 22:51:48 2011
  Status: Successfully committed 1004
```

Patch:

```
[edit system commit server]
+ days-to-keep-error-logs 4294967295;
  Id: 1007
  Last Modified: Wed Nov  2 01:08:04 2011
  Status: Successfully committed 1007
```

Patch:

```
[edit system commit server]
- days-to-keep-error-logs 4294967295;
+ days-to-keep-error-logs 2;
  Id: 1009
  Last Modified: Wed Nov  2 01:16:45 2011
  Status: Successfully committed 1009
```

Patch:

```
[edit]
+ snmp {
+   community abc;
+ }
  Id: 1010
  Last Modified: Wed Nov  2 01:19:25 2011
  Status: Successfully committed 1010
```

Patch:

```
[edit system syslog]
  file test { ... }
+ file j {
+   any any;
+ }
  Id: 1011
  Last Modified: Wed Nov  2 01:28:16 2011
  Status: Successfully committed 1011
```

Error commits:


```
Id: 1008
Last Modified: Wed Nov  2 01:08:18 2011
Status: Error while committing 1008
```

Patch:

```
[edit system]
+ radius-server {
```

```
+    10.1.1.1 port 222;  
+ }
```

show system commit server status

Syntax	show system commit server status
Release Information	Command introduced in Junos OS Release 12.1.
Description	Display commit server status.
	<div> NOTE: By default, the status of the commit server is “Not running”. The commit server starts running only when a commit job is added to the batch.</div>
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Batch Commit Server Properties on page 517
List of Sample Output	show system commit server status (When Server Is Inactive) on page 756 show system commit server status (When Server Is Active) on page 756

Sample Output

show system commit server status (When Server Is Inactive)

```
user@host> show system commit server status
Commit server status : Not running
```

show system commit server status (When Server Is Active)

```
user@R0> show system commit server status

Commit server status : Running
Jobs in process:
 1369 1370 1371
```

J-Web User Guide for Security Devices

PART 6

Overview

- [Understanding the J-Web User Interface on page 761](#)

Understanding the J-Web User Interface

- [J-Web Overview on page 761](#)
- [Starting the J-Web User Interface on page 762](#)
- [Understanding the J-Web Interface Layout on page 762](#)
- [Getting Help in the J-Web User Interface on page 765](#)

J-Web Overview

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI.

You can perform the following tasks with the J-Web interface:

- **Monitoring**—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- **Configuring**—The J-Web interface provides the following different configuration methods:
 - Configure the routing platform quickly and easily without configuring each statement individually.
 - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
 - Edit the configuration in a text file.
 - Upload a configuration file.

The J-Web interface also allows you to manage configuration history and set a rescue configuration.

- **Troubleshooting**—Troubleshoot routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic.

- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms.
- Configuring and monitoring events—Filter and view system log messages that record events occurring on the router. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.

Starting the J-Web User Interface

Before you start the user interface, you must perform the initial device configuration described in the Getting Started Guide for your device. After the initial configuration, you use your username and password, and the hostname or IP address of the device, to start the user interface.

To start the J-Web user interface:

1. Launch your HTTP-enabled or HTTPS-enabled Web browser.

To use HTTPS, you must have installed the certificate provided by the device.



NOTE: If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.

2. Type **http://** or **https://** in your Web browser followed by the hostname or IP address of the device, and press Enter.

The J-Web login page appears.

3. Type your username and password, and click **Log In**.

To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.



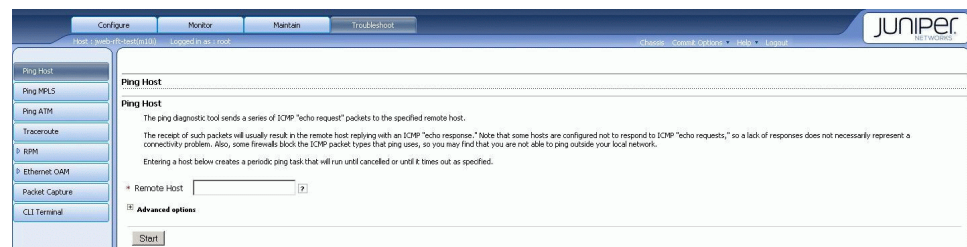
NOTE: The default username is **root** with no password. You must change this during initial configuration or the system does not accept the configuration.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

Understanding the J-Web Interface Layout

Each page of the J-Web interface is divided into the following panes, as shown in [Figure 24](#).

Figure 24: J-Web Layout

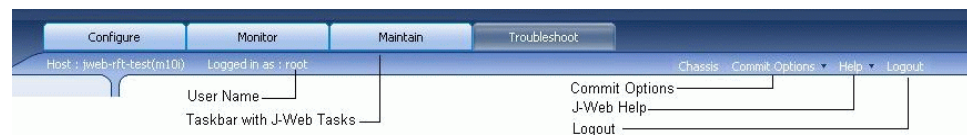


- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, troubleshoot, and manage the Juniper Networks device by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays subtasks of the Configure, Monitor, Maintain, or Troubleshoot task currently displayed in the main pane. For the configuration editor, this pane displays the hierarchy of configuration statements committed on the router. Click an item to access it in the main pane.

Top Pane

The top pane comprises the elements shown in Figure 25.

Figure 25: Top Pane Elements



- *hostname – model*—Hostname and model of the Juniper Networks device.
- Logged in as: *username*—Username you used to log in to the device.
- Chassis—The chassis view of the device.
- Commit Options
 - Commit—Commits the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be committed.
 - Compare—Displays the differences between the committed and uncommitted configuration on the device.
 - Discard—Discards the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be discarded.
 - Preference—Enables you to select preferences for committing configuration. **Commit Check** only validates the configuration and reports errors. **Commit** validates and commits the configuration specified on every J-Web page.
- Help
 - Help Contents—Link to context-sensitive help information.

- **About**—Link to information about the J-Web interface, such as the version number.
- **Logout**—Ends your current login session with the Juniper Networks device and returns you to the login page.
- **Taskbar**—Menu of J-Web tasks. Click a J-Web task to access it.
 - **Configure**—Configure the device by using Configuration pages or the configuration editor, and view configuration history.
 - **Monitor**—View information about configuration and hardware on the device.
 - **Maintain**—Manage files and licenses, upgrade software, and reboot the device.
 - **Troubleshoot**—Troubleshoot network connectivity problems.

Main Pane

The main pane comprises the elements shown in [Figure 26](#).

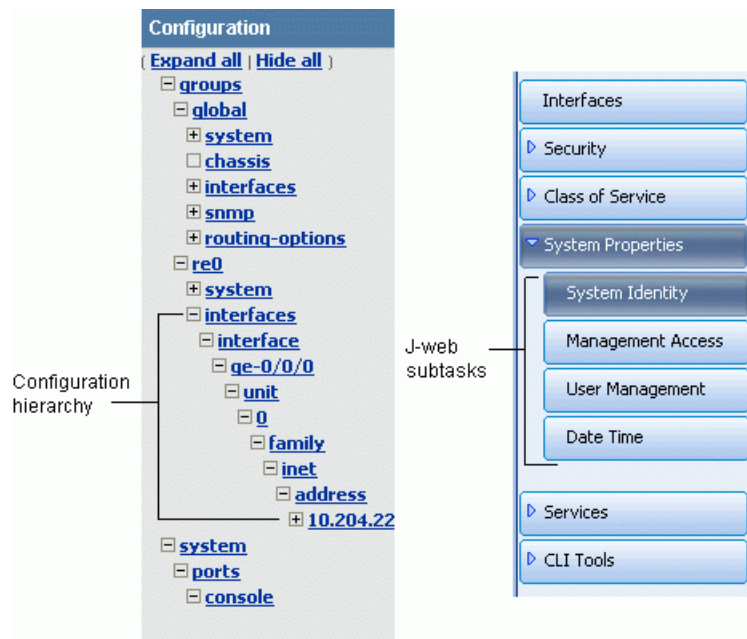
Figure 26: Main Pane Elements

- **Help (?) icon**—Displays useful information when you move the cursor over the question mark. This help displays field-specific information, such as the definition, format, and valid range of the field.
- **Red asterisk (*)**—Indicates a required field.

Side Pane

The side pane comprises the elements shown in [Figure 27](#).

Figure 27: Side Pane Elements



- Subtask—Displays options related to the selected task in the J-Web taskbar.
- Configuration hierarchy—For the J-Web configuration editor, displays the hierarchy of committed statements in the device configuration.
 - Click **Expand all** to display the entire hierarchy.
 - Click **Hide all** to display only the statements at the top level.
 - Click plus signs (+) to expand individual items.
 - Click minus signs (–) to hide individual items.

Getting Help in the J-Web User Interface

To get Help in the J-Web user interface, use the following methods:

- Field-sensitive Help—Move the cursor over the question mark (?) next to the field for which you want more information. Typically, this Help includes one line of information about what this field does or what you must enter in a given text box. For example, Help for the Peer Autonomous System Number text box states, “The value should be a number between 1 and 65535.”
- Context-sensitive Help—Click **Help** in the taskbar to open a separate page displaying the summary of all the fields on that page. To exit Help, close the page.
- Wizard Help (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650)—Use the Firewall Policy, VPN, and NAT wizards to perform basic configurations. Click a field in a wizard page to display information about that field in the lower-left corner of the wizard page.

PART 7

Configuring and Managing a Device Using J-Web

- [Installing J-Web on page 769](#)
- [Configuring Secure Web Access to a Device on page 771](#)
- [Configuring a Device Using J-Web on page 775](#)
- [Managing J-Web Sessions and Users on page 785](#)

Installing J-Web

- J-Web Software Requirements on page 769
- Installing the J-Web Software on page 769

J-Web Software Requirements

To access the J-Web interface for all platforms, your management device requires the following software:

- Supported browsers— Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0
- Language support— English-version browsers
- Supported OS— Microsoft Windows XP Service Pack 3

Other browser versions might not provide access to the J-Web interface.

Installing the J-Web Software

Your Juniper Networks device comes with the Junos OS installed on it. When you power on the Juniper device, all software starts automatically.

If your device is not shipped with the J-Web software on it, you must download the J-Web software package from the Juniper Networks webpage and install it on your device. After the installation, you must enable Web management of the device with the CLI.

To install and enable the J-Web software:

1. Using a Web browser, navigate to the Juniper Networks Customer Support Center at <https://www.juniper.net/customers/csc/software/>.
2. Log in to the Juniper Networks authentication system with the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Download the J-Web software to your local host. Select the version that is the same as the Junos OS version running on the device.
4. Copy the software package to the device. We recommend that you copy it to the `/var/tmp` directory.

5. If you have previously installed the J-Web software on the device, you must delete it before installing the new version. To do so, from operational mode in the CLI, enter the following command:

```
user@host> request system software delete jweb
```

6. Install the new package on the device. From operational mode in the CLI, enter the following command:

```
user@host> request system software add path/filename
```

Replace *path* with the full pathname to the J-Web software package. Replace *filename* with the filename of the J-Web software package.

7. Enable Web management of the device. From configuration mode in the CLI, enter the following command:

```
user@host# system services web-management http
```

CHAPTER 35

Configuring Secure Web Access to a Device

- [Secure Web Access Overview on page 771](#)
- [Generating SSL Certificates on page 771](#)
- [Configuring Secure Web Access on page 772](#)
- [Establishing J-Web Sessions on page 772](#)

Secure Web Access Overview

A Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure management of devices through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you are not able to access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

Generating SSL Certificates

To enable secure Web access, you must first generate a digital SSL certificate, and then enable HTTPS access on the Juniper Networks device.

To generate an SSL certificate:

1. Enter the following **openssl** command in your Secure Shell command-line interface. The **openssl** command generates a self-signed SSL certificate in the Privacy-Enhanced Mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
```

Replace **filename** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the **new.pem** file.

```
cat new.pem
```

Copy the contents of this file for installing the SSL certificate.

Go on to “[Configuring Secure Web Access](#)” on page 772 to install the SSL certificate and enable HTTPS.

Configuring Secure Web Access

Navigate to the Management Access Configuration page by selecting **Configure>System Properties>Management Access**. Click **Edit** from the main pane to open the Edit Management Access page. On this page, you can enable HTTP and HTTPS access on interfaces for managing Services Routers through the Web interface. You can also install SSL certificates and enable JUNOScript over SSL with the Secure Access page.

For more information, see *Help Contents* of this J-Web page.

Establishing J-Web Sessions

You establish a J-Web session through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the Junos OS. To use HTTPS, you must have installed the certificate provided by the device.

When you attempt to log in through the J-Web interface, the system authenticates your username with the same methods used for Telnet and SSH.

The device can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web *windows*—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

If the device does not detect any activity through the J-Web user interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

[Table 70](#) shows the maximum number of concurrent J-Web sessions on SRX Series devices.

Table 70: Concurrent Web Sessions on SRX Series Devices

Device Type	Maximum Number of Users
SRX300, SRX320, SRX340, SRX345, SRX1500	7
SRX5400, SRX5600, SRX5800	1024

CHAPTER 36

Configuring a Device Using J-Web

- [Configuring Basic Settings on page 776](#)
- [J-Web Configuration Pages Overview on page 778](#)
- [Editing a Configuration on page 779](#)
- [J-Web Commit Options Guidelines on page 782](#)
- [Committing a Configuration on page 783](#)

Configuring Basic Settings

Before you begin initial configuration, complete the following tasks:

- Install the Juniper Networks device in its permanent location, as described in the hardware installation guide or the Getting Started Guide for your device.
- Gather the following information:
 - Hostname for the router on the network
 - Domain that the router belongs to on the network
 - Password for the root user
 - Time zone where the router is located
 - IP address of a Network Time Protocol (NTP) server (if NTP is used to set the time on the router)
 - IP address of a Domain Name System (DNS) server
 - List of domains that can be appended to hostnames for DNS resolution
 - IP address of the default gateway
 - IP address to be used for the loopback interface
 - IP address of the built-in Ethernet interface that you will use for management purposes
- Collect the following equipment:
 - A management device, such as a laptop, with an Ethernet port
 - An Ethernet cable

To configure basic settings with J-Web Initial Configuration:

1. Enter information into the Initial Configuration Set Up page (see [Figure 28](#)), as described in [Table 71](#).
2. Click **Apply** to apply the configuration.

Figure 28: J-Web Set Up Initial Configuration Page

Initial Configuration

Set Up

Identification

* Host Name: ?

Domain Name: ?

* Root Password: ?

* Verify Root Password: ?

Time

Time Zone: ?

NTP Servers: ?

Current System Time: ?

?

?

Network

DNS Name Servers: ?

Domain Search: ?

Default Gateway:

Loopback Address: ?

fe-0/0/0.0 Address:

Management Access

The following access methods are considered insecure as any information sent over them will be sent without encryption and could possibly be intercepted during transmission.

Allow Telnet Access: ☒

Allow JUNOScript over Clear-Text Access: ☐

The following access method is considered secure as any information sent over it will be encrypted before transmission.

Allow SSH Access: ☒

In order to enable HTTPS or JUNOScript over SSL, you will need to visit the SSL configuration page to configure certificates and associations.

Table 71: Initial Configuration Set Up Summary

Field	Function	Your Action
Identification		
Host Name (required)	Defines the hostname of the router.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password (required)	Sets the root password that the user “root” can use to log in to the router.	Type a plain-text password that the system encrypts. NOTE: After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.
Verify Root Password (required)	Verifies that the root password has been typed correctly.	Retype the password.
Time		
Time Zone	Identifies the time zone that the router is located in.	From the list, select the appropriate time zone.
NTP Servers	Specify an NTP server that the router can reach to synchronize the system time.	To add an IP address, type it in the box to the left of the Add button, then click Add . To delete an IP address, click it in the box above the Add button, then click Delete .

Table 71: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
Current System Time	Synchronizes the system time with the NTP server, or manually sets the system time and date.	<ul style="list-style-type: none"> To immediately set the time using the NTP server, click Set Time via NTP. The router sends a request to the NTP server and synchronizes the system time. NOTE: If you are configuring other settings on this page, the router also synchronizes the system time using the NTP server when you click Apply. To set the time manually, click Set Time Manually. A pop-up window allows you to select the current date and time from lists.
Network		
DNS Name Servers	Specify a DNS server that the router can use to resolve hostnames into addresses.	<p>To add an IP address, type it in the box to the left of the Add button, then click Add.</p> <p>To delete an IP address, click it in the box above the Add button, then click Delete.</p>
Domain Search	Adds each domain name that the router is included in to the configuration so that they are included in a DNS search.	<p>To add a domain name, type it in the box to the left of the Add button, then click Add.</p> <p>To delete a domain name, click it in the box above the Add button, then click Delete.</p>
Default Gateway	Defines a default gateway through which to direct packets addressed to networks not explicitly listed in the routing table.	Type a 32-bit IP address, in dotted decimal notation.
Loopback Address	Defines a reserved IP address that is always available on the router. If no address is entered, this address is set to 127.0.0.1/32 .	Type a 32-bit IP address and prefix length, in dotted decimal notation.
Management Access		
Allow Telnet Access	Allows remote access to the router by using Telnet.	To enable Telnet access, select the check box.
Allow JUNOScript protocol over Clear-Text Access	Allows JUNOScript to access the router by using a protocol for sending unencrypted text over a TCP connection.	To enable JUNOScript access over clear text, select the check box.
Allow SSH Access	Allows remote access to the router by using SSH.	To enable SSH access, select the check box.

J-Web Configuration Pages Overview

J-Web configuration pages offer you several different ways to configure your Juniper Networks device. Configuration pages provide access to all the configuration statements

supported by the device, so you can fully configure it without using the CLI. You can also manage the configuration, monitor user access, and set a rescue configuration.

Table 72 provides a summary of the J-Web configuration pages.

Table 72: J-Web Configuration Pages Summary

J-Web Configuration Task	Description	More Information
Edit the configuration using a clickable interface	Expand the entire configuration hierarchy in the side pane and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option.	For more information, go to Configure>CLI Tools>Point and Click CLI in the J-Web user interface.
Edit the configuration in text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	For more information, go to Configure>CLI Tools>CLI Editor in the J-Web user interface.
Upload a configuration file	Upload a complete configuration.	For more information, go to Maintain>Config Management>Upload in the J-Web user interface.
View the configuration in text format	View the entire configuration on the device in text format.	For more information, go to Configure>CLI Tools>CLI Viewer in the J-Web user interface.

Editing a Configuration

To edit the configuration on a series of pages of clickable options that step you through the hierarchy, select **Configure>CLI Tools>Point and Click**. The side pane displays the top level of the configuration hierarchy, and the main pane displays configured hierarchy options and the Icon Legend (see Figure 29).

Figure 29: Edit Configuration Page

The screenshot displays the J-Web configuration editor interface. On the left, a sidebar shows a configuration hierarchy with 'Expand all' and 'Hide all' buttons. The main area is titled 'Configuration' and contains a list of configuration options, each with a 'Configure' link. The 'System' option is selected, showing fields for 'Access profile name' and 'Jsrc partition name'. Below these are advanced options for 'Apply groups' and an 'Icon Legend' section.

See the video for an example of how to use the J-Web configuration editor to configure and manage stateless firewall filters.



Video: Managing Firewall Filters with J-Web

To expand or hide the hierarchy of all the statements in the side pane, click **Expand all** or **Hide all**. To expand or hide an individual statement in the hierarchy, click the expand (+) or collapse (–) icon to the left of the statement.



NOTE: Only those statements included in the committed configuration are displayed in the side pane hierarchy.

The configuration information in the main pane consists of configuration options that correspond to configuration statements. Configuration options that contain subordinate statements are identified by the term *nested configuration*.

To include, edit, or delete statements in the candidate configuration, click one of the links described in [Table 73](#) in the main pane. Then specify configuration information by typing into a field, selecting a value from a list, or clicking a check box (toggle).

Table 73: J-Web Edit Configuration Links

Link	Function
Add new entry	Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.
Configure	Displays information for a configuration option that has not been configured, allowing you to include a statement.
Delete	Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.
Edit	Displays information for a configuration option that has already been configured, allowing you to edit a statement.
<i>identifier</i>	Displays fields and lists for an existing statement identifier, allowing you to edit the identifier.

As you navigate through the configuration, the hierarchy level is displayed at the upper right of the main pane. You can click a statement or identifier in the hierarchy to return to the corresponding configuration options in the main pane.

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. [Table 74](#) describes the meaning of these icons.

Table 74: J-Web Edit Configuration Icons

Icon	Meaning
C	Displays a comment about a statement.
I	Indicates that a statement is inactive.
M	Indicates that a statement has been added or modified, but has not been committed.
*	Indicates that the statement or identifier is required in the configuration.
?	Provides Help information.

J-Web Commit Options Guidelines

Using the J-Web Commit Preference, you can configure the commit options either to commit all global configurations together or to commit each configuration change immediately. Do one of the following to commit a configuration:

- Set Commit Preference to **Validate and commit configuration changes**, and then click **OK**.
- Set Commit Preference to **Validate configuration changes**, click **OK** to check your configuration and save it as a candidate configuration, and then click **Commit Options>Commit**.

For example, suppose you want to delete a firewall and add a new one.

- If Commit Preference is set to **Validate and commit configuration changes**, then you would need to commit your changes twice for each action.
- If Commit Preference is set to **Validate configuration changes**, then you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, allowing other users to edit those configurations, but the changes do not take effect on the device platform until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, changes made by all the users take effect.

You use the single commit feature to commit all your configurations in J-Web simultaneously. This helps to reduce the time J-Web takes to commit configurations because when changes are committed at every step, rollback configurations pile up quickly.



.....

NOTE: If you end a session with a particular Commit Preference, the subsequent sessions for that particular browser will automatically come up with the preference you previously selected. If you start the subsequent session on a different browser, the session will come up with the default commit preference.

.....



.....

NOTE: There are some pages whose configurations would need to be committed immediately. For such pages, even if you configure the commit options to perform a single global commit for them, the system displays appropriate information notification windows to remind you to commit your changes immediately. Examples of such pages are Switching, Interfaces, and Class of Service.

.....

Committing a Configuration

When you finish making changes to a candidate configuration with the J-Web configuration editor, you must commit the changes to use them in the current operational software running on the Juniper Networks device.

If another user is editing an exclusive candidate configuration with the CLI, you cannot commit a configuration until the user has committed the configuration. For more information about editing an exclusive candidate configuration, see the *Junos OS CLI User Guide*.

To commit a candidate configuration:

1. In the J-Web configuration editor, click **Commit**.

The main pane displays a summary of your changes in statement form.

2. To confirm the commit operation, click **OK**.

If multiple users are editing the configuration when you commit the candidate configuration, all changes made by all users take effect.

3. To display all the edits applied to the running configuration, click **Refresh**.

Managing J-Web Sessions and Users

- [Setting J-Web Session Limits on page 785](#)
- [Terminating J-Web Sessions on page 785](#)

Setting J-Web Session Limits

By default, an unlimited number of users can log in to the J-Web interface on a Juniper Networks device, and each session remains open for 24 hours (1440 minutes). Using CLI commands, you can limit the maximum number of simultaneous J-Web user sessions and set a default session timeout for all users.

- To limit the number of simultaneous J-Web user sessions, enter the following commands:

```
user@host# edit system services web-management session
user@host# set session-limit session-limit
```

Range: 1 through 1024. Default: Unlimited

- To change the J-Web session idle time limit, enter the following commands:

```
user@host# edit system services web-management session
user@host# set idle-timeout minutes
```

Range: 1 through 1440. Default: 1440

You can also configure the maximum number of simultaneous subordinate HTTP processes that the device creates in response to user requests.

To configure the maximum number of subordinate httpd processes, enter the following commands:

```
user@host# edit system services web-management limits
```

```
user@host# active-child-process process-limit
```

The default is 5, and the range is 0 through 32.

Terminating J-Web Sessions

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane. You must log in again to begin a new session.

By default, if the Juniper Networks device does not detect any activity through the J-Web interface for 24 hours, the session times out and is terminated. For information about changing the idle time limit, see [“Setting J-Web Session Limits” on page 785](#).

PART 8

Troubleshooting

- [Troubleshooting the J-Web User Interface on page 789](#)

CHAPTER 38

Troubleshooting the J-Web User Interface

- [Lost Router Connectivity on page 789](#)
- [Unpredictable J-Web Behavior on page 789](#)
- [No J-Web Access on page 789](#)

Lost Router Connectivity

- Problem** **Description:** After completing initial configuration, I lost connectivity to the Juniper device through J-Web.
- Cause** If you change the IP address of the management interface and have the management device configured to use DHCP, you lose your DHCP lease and your connection to the Juniper Networks device through the J-Web interface.
- Solution** To reestablish a connection, either set the IP address on the management device manually, or connect the management interface to the management network and access the Juniper device another way—for example, through the console port.

Unpredictable J-Web Behavior

- Problem** **Description:** I have multiple J-Web windows open and am experiencing unpredictable results.
- Solution** Close the extra windows. The Juniper Networks device can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web windows—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

No J-Web Access

- Problem** **Description:** I cannot access J-Web from my browser.
- Solution** **Solution 1**—On the Juniper Networks device, verify that you have successfully installed the J-Web software package and enabled Web management on the platform, as described in [“Installing the J-Web Software” on page 769](#).

Solution 2—If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the **Use SSL 3.0** option in the Web browser to access J-Web on the device.

Administration Guide for Security Devices

PART 9

User Access and Authentication

- [User Access and Authentication Overview on page 795](#)
- [Configuring Junos OS User Accounts on page 807](#)
- [Configuring User Access Privileges on page 829](#)
- [Permissions Flags for User Access Privileges on page 839](#)
- [Configuring Authentication Methods on page 1011](#)

User Access and Authentication Overview

- [Understanding Login Classes on page 795](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Understanding User Authentication Methods on page 804](#)
- [Hardening Shared Secrets in Junos OS on page 804](#)

Understanding Login Classes

All users who log in to the device must be in a login class. You can define any number of login classes. You then apply one login class to an individual user account. With login classes, you define the following:

- Access privileges users have when they are logged in to the device.
- Commands and statements that users can and cannot specify.
- How long a login session can be idle before it times out and the user is logged off.

You can define any number of login classes and then apply one login class to an individual user account.

[Table 75](#) contains a few predefined login classes. The predefined login classes cannot be modified.

Table 75: Predefined Login Classes

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
super-user and superuser	all
unauthorized	None

**NOTE:**

- You cannot modify a predefined login class name. If you issue the **set** command on a predefined class name, the Junos OS appends **-local** to the login class name. The following message also appears:

warning: '<class-name>' is a predefined class name; changing to '<class-name>-local'

- You cannot issue the **rename** or **copy** command on a predefined login class. Doing so results in the following error message:

error: target '<class-name>' is a predefined class

This section contains the following topics:

- [Permission Bits on page 796](#)
- [Denying or Allowing Individual Commands on page 798](#)

Permission Bits

Each top-level command-line interface (CLI) command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission bits (see [Table 76](#)).

Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 76: Permission Bits for Login Classes

Permission Bit	Access
admin	Can view user account information in configuration mode and with the show configuration command.
admin-control	Can view user accounts and configure them (at the [edit system login] hierarchy level).
access	Can view the access configuration in configuration mode and with the show configuration operational mode command.
access-control	Can view and configure access information (at the [edit access] hierarchy level).
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands).

Table 76: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
configure	Can enter configuration mode (using the configure command) and commit configurations (using the commit command).
control	Can perform all control-level operations (all operations configured with the -control permission bits).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the [edit firewall] hierarchy level).
floppy	Can read from and write to the removable media.
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the [edit] hierarchy).
maintenance	Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the device (using the request system commands).
network	Can access the network by entering the ping , ssh , telnet , and traceroute commands.
reset	Can restart software processes using the restart command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level).
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.

Table 76: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
security-control	Can view and configure security information (at the [edit security] hierarchy level).
shell	Can start a local shell on the device by entering the start shell command.
snmp	Can view SNMP configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the [edit system] hierarchy level).
trace	Can view trace file settings in configuration and operational modes.
trace-control	Can view trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics.

Denying or Allowing Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that are otherwise permitted or not allowed by a permission bit.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Template Accounts on page 810](#)
- [Example: Configuring New Users on page 807](#)

Understanding User Accounts

User accounts provide one way for users to access the device. Users can access the device without accounts if you configured RADIUS or TACACS+ servers. After you have created an account, the device creates a home directory for the user. An account for the user **root** is always present in the configuration. For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username.
- User's full name—If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- User identifier (UID)—Numeric identifier that is associated with the user account name. The identifier range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- User's access privilege—You can create login classes with specific permission bits or use one of the predefined classes.
- Authentication method or methods and passwords that the user can use to access the device—You can use SSH or an MD5 password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. If you configure the plain-text-password option, you are prompted to enter and confirm the password.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 1014](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)
- [Example: Configuring Authentication Order on page 1022](#)

Understanding Junos OS Access Privilege Levels

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more *permission flags*.

For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

The following sections provide additional information about permissions:

- [Junos OS Login Class Permission Flags on page 799](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 803](#)

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in [Table 77](#). Permission flags are not cumulative, so for each class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 77 lists the Junos OS login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level.

Table 77: Login Class Permission Flags

Permission Flag	Description
access	Can view the access configuration in configuration mode and with the show configuration operational mode command.
access-control	Can view and configure access information at the [edit access] hierarchy level.
admin	Can view user account information in configuration mode and with the show configuration operational mode command.
admin-control	Can view user accounts and configure them at the [edit system login] hierarchy level.
all-control	Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.
clear	Can clear (delete) information learned from the network that is stored in various network databases by using the clear commands.
configure	Can enter configuration mode by using the configure command.
control	Can perform all control-level operations—all operations configured with the -control permission flags.
field	Can view field debug commands. Reserved for debugging support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information at the [edit firewall] hierarchy level.
floppy	Can read from and write to the removable media.
flow-tap	Can view the flow-tap configuration in configuration mode.
flow-tap-control	Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap] hierarchy level.

Table 77: Login Class Permission Flags (*continued*)

Permission Flag	Description
flow-tap-operation	<p>Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must authenticate itself to the Junos OS as an administrative user. That account must have flow-tap-operation permission.</p> <p>NOTE: The flow-tap-operation option is not included in the all-control permissions flag.</p>
idp-profiler-operation	Can view profiler data.
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	<p>Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels:</p> <ul style="list-style-type: none"> • [edit chassis] • [edit class-of-service] • [edit groups] • [edit forwarding-options] • [edit interfaces]
maintenance	Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the su root command, and can halt and reboot the router or switch by using the request system commands.
network	Can access the network by using the ping , ssh , telnet , and traceroute commands.
pgcp-session-mirroring	Can view the pgcp session mirroring configuration.
pgcp-session-mirroring-control	Can modify the pgcp session mirroring configuration.
reset	Can restart software processes by using the restart command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level.
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.

Table 77: Login Class Permission Flags (*continued*)

Permission Flag	Description
routing-control	Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level.
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.
security-control	Can view and configure security information at the [edit security] hierarchy level.
shell	Can start a local shell on the router or switch by using the start shell command.
snmp	Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and can modify SNMP configuration at the [edit snmp] hierarchy level.
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it at the [edit system] hierarchy level.
trace	Can view trace file settings and configure trace file properties.
trace-control	Can modify trace file settings and configure trace file properties.
view	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.
view-configuration	<p>Can view all of the configuration excluding secrets, system scripts, and event options.</p> <p>NOTE: Only users with the maintenance permission can view commit script, op script, or event script configuration.</p>

Allowing or Denying Individual Commands for Junos OS Login Classes

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag. For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

- The **all** login class permission bits take precedence over extended regular expressions when a user with **rollback** permission issues the **rollback** command.
- Expressions used to allow and deny commands for users on RADIUS and TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (**allow-commands=cmd1 cmd2 ... cmdn**), you can specify each command as a separate expression. This new syntax is valid for **allow-configuration-regexps** and **deny-configuration-regexps**, **allow-commands** and **deny-commands**, and all user permission bits.
- Users cannot issue the **load override** command when specifying an extended regular expression. Users can only issue the **merge**, **replace**, and **patch** configuration commands.
- If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by the **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.
- Regular expressions for **allow-commands** and **deny-commands** can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

- Related Documentation**
- [Configuring Access Privilege Levels on page 829](#)
 - [Access Privilege User Permission Flags Overview on page 840](#)

Understanding User Authentication Methods

Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the device.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the device using Telnet. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the device, and the server runs on a remote network system.

You can configure the device to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the device. If you set up both authentication methods, you also can configure which method the device will try first.

- Related Documentation**
- [Understanding User Accounts on page 798](#)
 - [Understanding Login Classes on page 795](#)
 - [Understanding Template Accounts on page 810](#)
 - [Example: Configuring Authentication Order on page 1022](#)
 - [Example: Configuring a RADIUS Server for System Authentication on page 1014](#)
 - [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)

Hardening Shared Secrets in Junos OS

- [Understanding Hardening Shared Secrets on page 804](#)

Understanding Hardening Shared Secrets

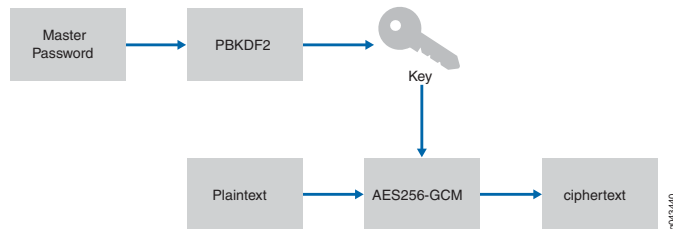
Existing shared secrets (\$9\$ format) in Junos OS currently use an obfuscation algorithm, which is not a very strong encryption for configuration secrets. If you want a strong encryption for your configuration secrets, you can configure a master password. The master password is used to derive an encryption key that is used with AES256-GCM to

encrypt configuration secrets. This new encryption method uses the `8` formatted strings.

Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password. The master password encrypts secrets like the RADIUS password, IKE preshared keys, and other shared secrets in the Junos OS management process (mgd) configuration. The master password itself is not saved as part of the configuration. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. the key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text). See [Figure 30](#)

Figure 30: Master Password Encryption



The `8` configuration secrets can only be shared between devices using the same master password.

The `8`-encrypted passwords have the following format:

`8crypt-algo$hash-algo$iterations$salt$ivtagencrypted`. See [Table 78](#) for the master password format details.

Table 78: `8`-encrypted Password Format

Format	Description
crypt-algo	Encryption/decryption algorithm to be used. Currently only AES256-GCM is supported.
hash-algo	Hash (prf) algorithm to be used for the PBKDF2 key derivation.
iterations	The number of iterations to use for the PBKDF2 hash function. Current iteration-count default is 100. The iteration count slows the hashing count, thus slowing attacker guesses.
salt	Sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used to <i>salt</i> (a random, but known string) the password and input to the PBKDF2 key derivation.
iv	A sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used as initialization vector for the AES256-GCM encryption function.
tag	ASCII64-encoded representation of the tag.

Table 78: \$8\$-encrypted Password Format (*continued*)

encrypted	ASCII64-encoded representation of the encrypted password.
-----------	---

The ASCII64 encoding is Base64 (RFC 4648) compatible, except no padding (character “=”) is used to keep the strings short. For example:
\$8\$aes256-gcm\$hmhac-sha2-256\$100\$y/4YMC4YDLU\$FzYDI4jjiN6YCyQsYLsaf8A\$llu4jLcZarD9YnyD
/Hejww\$okhBlc0cGakSqYxKww

Chassis Cluster Considerations

When defining a chassis cluster on SRX Series devices, be aware of the following restrictions:

- For SRX Series devices, first configure the master password on each node, and then build the cluster. The same master password should be configured on each node.
- In chassis cluster mode, the master password cannot be deleted.



NOTE: A change in the master password would mean disruption in chassis clustering; therefore you must change the password on both nodes independently.

CHAPTER 40

Configuring Junos OS User Accounts

- [Example: Configuring New Users on page 807](#)
- [Understanding Template Accounts on page 810](#)
- [Example: Creating Template Accounts on page 810](#)
- [Understanding Administrative Roles on page 813](#)
- [Example: Configuring Administrative Roles on page 815](#)
- [Handling Authorization Failure on page 822](#)
- [Example: Configuring System Retry Options on page 823](#)

Example: Configuring New Users

This example shows how to configure new users.

- [Requirements on page 807](#)
- [Overview on page 807](#)
- [Configuration on page 808](#)
- [Verification on page 810](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can add new users to the device's local database. For each account, you define a login name and password for the user and specify a login class for access privileges. The login password must meet the following criteria:

- The password must be at least six characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), but not control characters.
- The password must contain at least one change of case or character class.

In this example, you create a login class named `operator-and-boot` and allow it to reboot the device. You can define any number of login classes. You then allow the

operator-and-boot login class to use commands defined in the clear, network, reset, trace, and view permission bits.

Then you create user accounts. User accounts provide enable you to access the device. (You can access the device without accounts if you configured RADIUS or TACACS+ servers.) You set the username as cmartin and the login class as superuser. Finally, you define the encrypted password for the user.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class operator-and-boot allow-commands "request system reboot"
set class system login operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password
$1$ABC123
```

GUI Step-by-Step Procedure

To configure new users:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Users** tab.
4. Click **Add** to add a new user. The Add User dialog box appears.
5. In the User name box, type a unique name for the user.

Do not include spaces, colons, or commas in the username.

6. In the User ID box, type a unique ID for the user.
7. In the Full Name box, type the user's full name.

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.
9. From the Login Class list, select the user's access privilege:

- **operator**
- **read-only**
- **unauthorized**

This list also includes any user-defined login classes.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

```
[edit system login]
user@host# set class operator-and-boot allow-commands "request system reboot"
```

2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace
view]
```

3. Set the username, login class, and encrypted password for the user.

```
[edit system login]
user@host# set user cmartin class superuser authentication encrypted-password
$1$ABC123
```

Results From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
class operator-and-boot {
permissions [ clear network reset trace view ];
allow-commands "request system reboot";
}
user cmartin {
class superuser;
authentication {
encrypted-password "$1$ABC123";
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 1014](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 1019](#).
- Configure a user. See [“Example: Configuring New Users” on page 807](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 810](#).

Verification

Confirm that the configuration is working properly.

Verifying the New Users Configuration

Purpose Verify that the new users have been configured.

Action From operational mode, enter the **show system login** command.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Template Accounts on page 810](#)
- [Understanding Login Classes on page 795](#)

Understanding Template Accounts

You use local user template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the device and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, Junos OS issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the device, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, the device selects the appropriate local user template locally configured on the device. If a local user template does not exist for the authenticated user, the device defaults to the **remote** template.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Login Classes on page 795](#)
- [Example: Creating Template Accounts on page 810](#)

Example: Creating Template Accounts

This example shows how to create template accounts.

- [Requirements on page 811](#)
- [Overview on page 811](#)
- [Configuration on page 811](#)
- [Verification on page 813](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

By default, Junos OS uses the **remote** template account when:

- The authenticated user does not exist locally on the device.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

In this example, you create a remote template account and set the username to remote and the login class for the user as operator. You create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

Configuration

- [Creating a Remote Template Account on page 811](#)
- [Creating a Local Template Account on page 812](#)

Creating a Remote Template Account

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user remote class operator
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To create a remote template account:

- Set the username and the login class for the user.

```
[edit system login]
user@host# set user remote class operator
```

Results From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
user remote {
class operator;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Creating a Local Template Account

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user admin class superuser
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To create a local template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user admin class superuser
```

Results From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
user admin {
class super-user;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a system authentication order. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 1014.](#)
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 1019.](#)
- Configure system authentication order. See [“Example: Configuring Authentication Order” on page 1022.](#)

Verification

Confirm that the configuration is working properly.

Verifying the Template Accounts Creation

Purpose Verify that the template accounts have been created.

Action From operational mode, enter the **show system login** command.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Login Classes on page 795](#)
- [Understanding Template Accounts on page 810](#)

Understanding Administrative Roles

A system user can be a member of a class that allows the user to act as a particular kind of administrator for the system. Requiring a specific role to view or modify an item restricts the extent of information a user can obtain from the system. It also limits how much of the system is open to intentional or unintentional modification or observation by a user. We recommend that you use the following guidelines when you are designing administrative roles:

- Do not allow any user to log in to the system as **root**.
- Restrict each user to the smallest set of privileges needed to perform the user's duties.
- Do not allow any user to belong to a login class containing the **shell** permission flag. The **shell** permission flag allows users to run the **start shell** command from the CLI.
- Allow users to have rollback permissions. Rollback permissions allow users to undo an action performed by an administrator but does not allow them to commit the changes.

You can assign an administrative role to a user by configuring a login class to have the privileges required for that role. You can configure each class to allow or deny access to configuration statements and commands by name. These specific restrictions override and take precedence over any permission flags also configured in the class. You can assign one of the following role attributes to an administrative user.

- **Crypto-administrator**—Allows the user to configure and monitor cryptographic data.
- **Security-administrator**—Allows the user to configure and monitor security data.
- **Audit-administrator**—Allows the user to configure and monitor audit data.
- **IDS-administrator**—Allows the user to monitor and clear the intrusion detection service (IDS) security logs.

Each role can perform the following specific management functions:

- **Cryptographic Administrator**
 - Configures the cryptographic self-test.
 - Modifies the cryptographic security data parameters.
- **Audit Administrator**
 - Configures and deletes the audit review search and sort feature.
 - Searches and sorts audit records.
 - Configures search and sort parameters.
 - Manually deletes audit logs.
- **Security Administrator**
 - Invokes, determines, and modifies the cryptographic self-test behavior.
 - Enables, disables, determines, and modifies the audit analysis and audit selection functions and configures the device to automatically delete audit logs.
 - Enables or disables security alarms.
 - Specifies limits for quotas on Transport Layer connections.
 - Specifies the limits, network identifiers, and time periods for quotas on controlled connection-oriented resources.
 - Specifies the network addresses permitted to use Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP).
 - Configures the time and date used in time stamps.
 - Queries, modifies, deletes, and creates the information flow or access control rules and attributes for the unauthenticated information flow security function policy (SFP), the authenticated information flow SFP, the unauthenticated device services, and the discretionary access control policy.
 - Specifies initial values that override default values when object information is created under unauthenticated information flow SFP, the authenticated information flow

SFP, the unauthenticated target of evaluation (TOE) services, and the discretionary access control policy.

- Creates, deletes, or modifies the rules that control the address from which management sessions can be established.
- Specifies and revokes security attributes associated with the users, subjects, and objects.
- Specifies the percentage of audit storage capacity at which the device alerts administrators.
- Handles authentication failures and modifies the number of failed authentication attempts through SSH or from the CLI that can occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.
- Manages basic network configuration of the device.
- **IDS Administrator**—Specifies IDS security alarms, intrusion alarms, audit selections, and audit data.

You need to set the security-role attribute in the classes created for these administrative roles. This attribute restricts which users can show and clear the security logs, actions that cannot be performed through configuration alone.

For example, you need to set the security-role attribute in the **ids-admin** class created for the IDS administrator role if you want to restrict clearing and showing IDS logs to the IDS administrator role. Likewise, you need to set the security-role to one of the other admin values to restrict that class from being able to clear and show non-IDS logs only.



NOTE: When a user deletes an existing configuration, the configuration statements under the hierarchy level of the deleted configuration (that is, the child objects that the user does not have permission to modify), now remain in the device.

Related Documentation

- [Example: Configuring Administrative Roles on page 815](#)

Example: Configuring Administrative Roles

This example shows how to configure individual administrative roles for a distinct, unique set of privileges apart from all other administrative roles.

- [Requirements on page 816](#)
- [Overview on page 816](#)
- [Configuration on page 816](#)
- [Verification on page 821](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

This example configures four users:

- **audit-officer** of the class **audit-admin**
- **crypto-officer** of the class **crypto-admin**
- **security-officer** of the class **security-admin**
- **ids-officer** of the class **ids-admin**

When a **security-admin** class is configured, the privileges for creating administrators are revoked from the user who created the **security-admin** class. Creation of new users and logins is at the discretion of the **security-officer**.

In this example, you create audit admin, crypto admin, security admin, and ids admin with permission flags pertaining to this role. Then you allow or deny access to configuration statements and commands by name for each administrative role. These specific restrictions take precedence over the permission flags also configured in the class. For example, only the **crypto-admin** can run the **request system set-encryption-key** command, which requires having the **security** permission flag to access it. Only the **security-admin** can include the **system time-zone** statement in the configuration, which requires having the **system-control** permission flag.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class audit-admin permissions security
set system login class audit-admin permissions trace
set system login class audit-admin permissions maintenance
set system login class audit-admin allow-commands "^clear (log|security log)"
set system login class audit-admin deny-commands "^clear (security alarms|system
login lockout)|^file (copy|delete|rename)|^request (security|system
set-encryption-key)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell";
set system login class audit-admin security-role audit-administrator
set system login class crypto-admin permissions admin-control
set system login class crypto-admin permissions configure
set system login class crypto-admin permissions maintenance
set system login class crypto-admin permissions security-control
set system login class crypto-admin permissions system-control
set system login class crypto-admin permissions trace
set system login class crypto-admin allow-commands "^request system
set-encryption-key"
```



```

set system login class crypto-admin deny-commands "^clear (log|security alarms|security
log|system login logout)|^file (copy|delete|rename)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
set system login class crypto-admin allow-configuration-regexps "security (ike|ipsec)
(policy|proposal)" "security ipsec ^vpn$ .* manual
(authentication|encryption|protocol|spi)" "system fips self-test after-key-generation"
set system login class crypto-admin security-role crypto-administrator
set system login class security-admin permissions all
set system login class security-admin deny-commands "^clear (log|security
log)|^(clear|show) security alarms alarm-type idp|^request (security|system
set-encryption-key)|^rollback|^start shell"
set system login class security-admin deny-configuration-regexps "security alarms
potential-violation idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$
.* manual (authentication| encryption|protocol|spi)" "security log cache" "security log
exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
set system login class security-admin security-role security-administrator
set system login class ids-admin permissions configure
set system login class ids-admin permissions security-control
set system login class ids-admin permissions trace
set system login class ids-admin permissions maintenance
set system login class ids-admin allow-configuration-regexps "security alarms
potential-violation idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^ (clear|show) security
alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show) security
alarms alarm-type
(authentication|cryptographic-self-test|decryption-failures|encryption-failures|
ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^file (copy|delete|rename)|^request
(security|system set-encryption-key)|^rollback|
^set date|^show security (dynamic-policies|match-policies|policies)|^start shell"
set system login class ids-admin deny-configuration-regexps "security alarms
potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
set system login class ids-admin security-role ids-admin
set system login user audit-officer class audit-admin
set system login user crypto-officer class crypto-admin
set system login user security-officer class security-admin
set system login user ids-officer class ids-admin
set system login user audit-officer authentication plain-text-password
set system login user crypto-officer authentication plain-text-password
set system login user security-officer authentication plain-text-password
set system login user ids-officer authentication plain-text-password

```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To configure users in administrative roles:

1. Create the **audit-admin** login class.

```

[edit]
user@host# set system login class audit-admin
[edit system login class audit-admin]

```

```

user@host# set permissions security
user@host# set permissions trace
user@host# set permissions maintenance

```

2. Configure the **audit-admin** login class restrictions.

```

[edit system login class audit-admin]
user@host# set allow-commands "^clear (log|security log)"
user@host# set deny-commands "^clear (security alarms|system login logout)|^file
(copy|delete|rename)|^request (security|system
set-encryption-key)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set security-role audit-administrator

```

3. Create the **crypto-admin** login class.

```

[edit]
user@host# set system login class crypto-admin

```

```

[edit system login class crypto-admin]
user@host# set permissions admin-control
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions system-control
user@host# set permissions trace

```

4. Configure the **crypto-admin** login class restrictions.

```

[edit system login class crypto-admin]
user@host# set allow-commands "^request system set-encryption-key"
user@host# set deny-commands "^clear (log|security alarms|security log|system
login logout)|^file (copy|delete|rename)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set allow-configuration-regexps "security (ike|ipsec) (policy|proposal)"
"security ipsec ^vpn$.* manual (authentication|encryption|protocol|spi)" "system
fips self-test after-key-generation"
user@host# set security-role crypto-administrator

```

5. Create the **security-admin** login class.

```

[edit]
user@host# set system login class security-admin

```

```

[edit system login class security-admin]
user@host# set permissions all

```

6. Configure the **security-admin** login class restrictions.

```

[edit system login class security-admin]
user@host# set deny-commands "^clear (log|security log)|^(clear|show) security
alarms alarm-type idp|^request (security|system
set-encryption-key)|^rollback|^start shell"
user@host# set deny-configuration-regexps "security alarms potential-violation
idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$.* manual
(authentication| encryption|protocol|spi)" "security log cache" "security log
exclude.* event-id IDP_.*" "system fips self-test after-key- generation"
user@host# set security-role security-administrator

```

7. Create the **ids-admin** login class.

```
[edit]
user@host# set system login class ids-admin
```

```
[edit system login class ids-admin]
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the **ids-admin** login class restrictions.

```
[edit system login class ids-admin]
user@host# set allow-configuration-regexps "security alarms potential-violation
idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^ (clear|show) security
alarms (alarm-id|all|newer-than|older- than|process|severity)|^ (clear|show)
security alarms alarm-type
(authentication|cryptographic-self-test|decryption-failures|encryption-failures|
ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^ file
(copy|delete|rename)|^ request (security|system set-encryption-key)|
^rollback|^set date|^show security (dynamic-policies|match-policies|policies)|^start
shell"
set system login class ids-admin deny-configuration-regexps "security alarms
potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
user@host# set security-role ids-administrator
```

9. Assign users to the roles.

```
[edit]
user@host# set system login

[edit system login]
user@host# set user audit-officer class audit-admin
user@host# set user crypto-officer class crypto-admin
user@host# set user security-officer class security-admin
user@host# set user ids-officer class ids-admin
```

10. Configure passwords for the users.

```
[edit system login]
user@host# set user audit-officer authentication plain-text-password
user@host# set user crypto-officer authentication plain-text-password
user@host# set user security-officer authentication plain-text-password
user@host# set user ids-officer authentication plain-text-password
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

[edit]
user@host# show system
system {
  login {
    class audit-admin {
      permissions [ maintenance security trace ];
      allow-commands "^clear (log|security log)";
      deny-commands "^clear (security alarms|system login logout)|^file
        (copy|delete|rename)|^request (security|system
        set-encryption-key)|^rollback|^set date|^show security
        (alarms|dynamic-policies|match-policies|policies)|^start shell";
      security-role audit-administrator;
    }
    class crypto-admin {
      permissions [ admin-control configure maintenance security-control system-control
        trace ];
      allow-commands "^request (system set-encryption-key)";
      deny-commands "^clear (log|security alarms|security log|system login logout)|^file
        (copy|delete|rename)|^rollback|^set date|^show security
        (alarms|dynamic-policies|match-policies|policies)|^start shell";
      allow-configuration-regexps "security (ike|ipsec) (policy|proposal)" "security ipsec
        ^vpn$.* manual (authentication|encryption|protocol|spi)" "system fips self-test
        after-key-generation" ;
      security-role crypto-administrator;
    }
    class security-admin {
      permissions [ all];
      deny-commands "^clear (log|security log)|^(clear|show) security alarms alarm-type
        idp|^request (security|system set-encryption-key)|^rollback|^start shell";
      deny-configuration-regexps "security alarms potential-violation idp" "security
        (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$.* manual
        (authentication|encryption|protocol|spi)" "security log exclude.* event-id IDP_.*"
        "system fips self-test after-key-generation";
      security-role security-administrator;
    }
    class ids-admin {
      permissions [ configure maintenance security-control trace ];
      deny-commands "^clear log|^(clear|show) security alarms
        (alarm-id|all|newer-than|older-than|process|severity)|^(clear|show) security
        alarms alarm-type
        (authentication | cryptographic-self-test | decryption-failures | encryption-failures
        | ike-phase1-failures | ike-phase2-failures|key-generation-self-test |
        non-cryptographic-self-test |policy | replay-attacks) | ^file (copy|delete|rename)
        |^request (security|system set-encryption-key) | ^rollback |
        ^set date | ^show security (dynamic-policies|match-policies|policies) |^start shell";
      allow-configuration-regexps "security alarms potential-violation idp" "security log
        exclude.* event-id IDP_.*";
      deny-configuration-regexps "security alarms potential-violation
        (authentication|cryptographic-self-test|decryption-
        failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
        key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
      security-role ids-administrator;
    }
  }
  user audit-officer {
    class audit-admin;
    authentication {

```

```

        encrypted-password "$1$ABC123"; ## SECRET-DATA
    }
}
user crypto-officer {
    class crypto-admin;
    authentication {
        encrypted-password "$1$ABC123."; ## SECRET-DATA
    }
}
user security-officer {
    class security-admin;
    authentication {
        encrypted-password "$1$ABC123."; ##SECRET-DATA
    }
}
user ids-officer {
    class ids-admin;
    authentication {
        encrypted-password "$1$ABC123/"; ## SECRET-DATA
    }
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Login Permissions

Purpose Verify the login permissions for the current user.

Action From operational mode, enter the **show cli authorization** command.

```

user@host>show cli authorization
Current user: 'example' class 'super-user'
Permissions:
  admin      -- Can view user accounts
  admin-control-- Can modify user accounts
  clear      -- Can clear learned network info
  configure  -- Can enter configuration mode
  control    -- Can modify any config
  edit       -- Can edit full files
  field      -- Can use field debug commands
  floppy     -- Can read and write the floppy
  interface  -- Can view interface configuration
  interface-control-- Can modify interface configuration
  network    -- Can access the network
  reset      -- Can reset/restart interfaces and daemons
  routing    -- Can view routing configuration
  routing-control-- Can modify routing configuration
  shell      -- Can start a local shell
  snmp       -- Can view SNMP configuration
  snmp-control-- Can modify SNMP configuration
  system     -- Can view system configuration

```

```

system-control-- Can modify system configuration
trace          -- Can view trace file settings
trace-control-- Can modify trace file settings
view           -- Can view current values and statistics
maintenance   -- Can become the super-user
firewall       -- Can view firewall configuration
firewall-control-- Can modify firewall configuration
secret         -- Can view secret statements
secret-control-- Can modify secret statements
rollback       -- Can rollback to previous configurations
security       -- Can view security configuration
security-control-- Can modify security configuration
access         -- Can view access configuration
access-control-- Can modify access configuration
view-configuration-- Can view all configuration (not including secrets)
flow-tap       -- Can view flow-tap configuration
flow-tap-control-- Can modify flow-tap configuration
idp-profiler-operation-- Can Profiler data
pgcp-session-mirroring-- Can view pgcp session mirroring configuration
pgcp-session-mirroring-control-- Can modify pgcp session mirroring configuration
storage        -- Can view fibre channel storage protocol configuration
storage-control-- Can modify fibre channel storage protocol configuration
all-control    -- Can modify any configuration
Individual command authorization:
Allow regular expression: none
Deny regular expression: none
Allow configuration regular expression: none
Deny configuration regular expression: none

```

This output summarizes the login permissions.

Related Documentation • [Understanding Administrative Roles on page 813](#)

Handling Authorization Failure

The security administrator can configure the number of times a user can try to log in to the device with invalid login credentials. The device can be locked after the specified number of unsuccessful authentication attempts. This helps to protect the device from malicious users attempting to access the system by guessing an account's password. The security administrator can unlock the user account or define a time period for the user account to remain locked.

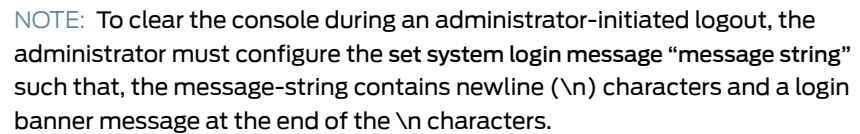
The system **lockout-period** defines the amount of time the device can be locked for a user account after a specified number of unsuccessful login attempts.

The security administrator can configure a period of time after which an inactive session will be locked and require re-authentication to be unlocked. This helps to protect the device from being idle for a long period before the session times out.

The system **idle-timeout** defines length of time the CLI operational mode prompt remains active before the session times out.

The security administrator can configure a banner with an advisory notice to be displayed before the identification and authentication screen.

The number of reattempts the device allows is defined by the **tries-before-disconnect** option. The device allows 3 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console.

[illegible]

- [Example: Configuring System Retry Options on page 823](#)

- Requirements on page 823
- Overview on page 823
- Configuration on page 826
- Verification on page 827

Overview

823

Device lockout allows you to configure the number of failed attempts before the user account is locked out of the device and configure the amount of time before the user can attempt to log in to the device again. You can configure the amount of time in-between failed login attempts of a user account and can manually lock and unlock user accounts.

**NOTE:**

This example includes the following settings:

- **backoff-factor** — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the **backoff-threshold** statement. The default value for this statement is five seconds, with a range of five to ten seconds.
- **backoff-threshold** — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the **backoff-factor** statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.
- **lockout-period** — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.
- **tries-before-disconnect** — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH or Telnet. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the **lockout-period** statement before attempting to log back in to the device. The **tries-before-disconnect** statement must be set when the **lockout-period** statement is set; otherwise, the **lockout-period** statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

Once a user is locked out of the device, if you are the security administrator, you can manually remove the user from this state using the `clear system login lockout <username>` command. You can also use the `show system login lockout` command to view which users are currently locked out, when the lockout period began for each user, and when the lockout period ends for each user.

If the security administrator is locked out of the device, he can log in to the device from the console port, which ignores any user locks. This provides a way for the administrator to remove the user lock on their own user account.

In this example the user waits for the **backoff-threshold** multiplied by the **backoff-factor** interval, in seconds, to get the login prompt. In this example, the user must wait 5 seconds after the first failed login attempt and 10 seconds after the second failed login attempt to get the login prompt. The user gets disconnected after 15 seconds after the third failed attempt because the **tries-before-disconnect** option is configured as 3.

The user cannot attempt another login until 120 minutes has elapsed, unless a security administrator manually clears the lock sooner.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login retry-options backoff-factor 5
set system login retry-options backoff-threshold 1
set system login retry-options lockout-period 120
set system login retry-options tries-before-disconnect 3
```

Step-by-Step Procedure To configure system retry-options:

1. Configure the backoff factor.

```
[edit]
user@host# set system login retry-options backoff-factor 5
```
2. Configure the backoff threshold.

```
[edit]
user@host# set system login retry-options backoff-threshold 1
```
3. Configure the amount of time the device gets locked after failed attempts.

```
[edit]
user@host# set system login retry-options lockout-period 5
```
4. Configure the number of unsuccessful attempts during which, the device can remain unlocked.

```
[edit]
user@host# set system login retry-options tries-before-disconnect 3
```

Results From configuration mode, confirm your configuration by entering the **show system login retry-options** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 5;
tries-before-disconnect 3;
```

Confirm that the configuration is working properly.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Displaying the Locked User Logins

Purpose Verify that the login lockout configuration is enabled.

Action Attempt three unsuccessful logins for a particular username. The device will be locked for that username; then log in to the device with a different username. From operational mode, enter the **show system login lockout** command.

Meaning When you perform three unsuccessful login attempts with a particular username, the device is locked for that user for five minutes, as configured in the example. You can verify that the device is locked for that user by logging in to the device with a different username and entering the **show system login lockout** command.

Related Documentation

- [Handling Authorization Failure on page 822](#)

Configuring User Access Privileges

- [Configuring Access Privilege Levels on page 829](#)
- [Example: Configuring User Permissions with Access Privilege Levels on page 830](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 833](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 835](#)

Configuring Access Privilege Levels

Each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges.

To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
permissions [ permissions ];
```

Related Documentation

- [Example: Configuring User Permissions with Access Privilege Levels on page 830](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- *permissions*

Example: Configuring User Permissions with Access Privilege Levels

Create two access privilege classes on the router or switch, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

In this example, you create two custom login classes on the router or switch and assign access privileges to each class through permission flags. The first custom login class is called **user-accounts** and it only includes access privileges for configuring and viewing user accounts. The second custom login class is called **network-mgmt** and only includes access privileges for configuring SNMP parameters.

```
[edit]
system {
  login {
    class user-accounts {
      permissions [ configure admin admin-control ];
    }
    class network-mgmt {
      permissions [ configure snmp snmp-control ];
    }
  }
}
```

1. Create the **user-accounts** custom login class and give it control over user accounts with the **configure admin admin-control** permission flag.

```
[edit system login]
user@router# set class user-accounts permissions configure admin admin-control
```

2. Create the **network-mgmt** custom login class and use the **configure snmp snmp-control** permission flag to assign it SNMP configuration privileges.

```
[edit system login]
user@router# set class network-mgmt permissions configure snmp snmp-control
```

3. Check your configuration by using the **show system login** command.

```
user@router# show system login
class user-accounts {
  permissions [ configure admin admin-control ];
}
class network-mgmt {
  permissions [ configure snmp snmp-control ];
}
```

Related Documentation

- [Configuring Access Privilege Levels on page 829](#)

Specifying Access Privileges for Junos OS Operational Mode Commands

You can specify extended regular expressions by using the **allow-commands** and **deny-commands** statements to define a user's access privileges to individual operational mode commands. Doing so takes precedence over a login class permissions bit set for a user. You can include one **deny-commands** and one **allow-commands** statement in each login class.

To explicitly provide use of an individual operational mode command that would otherwise be denied, include the **allow-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
  allow-commands "regular-expression";
```

To explicitly deny access to an individual operational mode command that would otherwise be supported, include the **deny-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
  deny-commands "regular-expression";
```



NOTE: The regular expression to allow/deny commands for any login class is supported at the command level but not at the argument level. For example, you can completely block ping but not ping *argument1*.

If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive.

```
allow-commands "show interfaces";
```



NOTE: Modifiers are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

For example, the deny command **set protocols** does not match anything, whereas **protocols** matches *protocols*.

Explicitly providing access to operational mode commands using the **allow-commands** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying access to operational mode commands using the **deny-commands** statement removes permissions for the specified commands from the default permissions provided by the **permissions** statement.

For example, if a login class has the permission **view** and the **allow-commands** statement includes the **request system software add** command, the specified login class user can install software, in addition to the permissions specified by the **view** permissions flag. Likewise, if a login class has the permission **all** and the **deny-commands** statement includes the **request system software add** command, the specified login class user can perform all operations allowed by the **all** permissions flag, except installing software using the **request system software add** command.

If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.

If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **deny-commands**.

Anchors are required when specifying complex regular expressions with **allow-commands** or **deny-commands** statements. For example, when specifying multiple commands using the pipe (|) symbol for **allow-commands**, the following syntax is incorrect:

allow-commands = "(monitor.*)"|(ping.*)"|(show.*)"|(exit)" . Instead, you must specify the expression using the following syntax: **allow-commands = "(^monitor) | (^ping) | (^show) | (^exit)"** OR **allow-commands = "^ (monitor | ping | show | exit)"**

**Related
Documentation**

- [Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 833](#)
- *Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands*
- *allow-commands*
- *deny-commands*

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands

Each operational mode command has an access privilege level associated with it. Access privileges control the commands that each custom login class can execute, configure, and view. Custom login classes are groups of users who are assigned with customized levels of access to different commands and statements. This ensures that each group of users can only use commands appropriate to their function, preventing unauthorized users from executing sensitive commands that could potentially cause damage to the network.

In this example, you create three custom login classes on the router or switch and assign access privileges for operational mode commands through the **allow-commands** and **deny-commands** settings. Each custom login class uses the same set of permission flags as the default login class **operator**, but **the login class is** allowed or denied certain operational mode commands. The first custom login class is called **operator-and-boot** and it has access to the **request system reboot** operational mode command. The second custom login class is called **operator-no-set** and it is denied access to any **set** commands. The third login class is called **operator-and-install-but-no-bgp** and it has access to the **request system software add** and **show route** operational mode commands, but it is denied access to the **show bgp** command.

```
[edit]
system {
  login {
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    class operator-no-set {
      permissions [ clear network reset trace view ];
      deny-commands "set";
    }
    class operator-and-install-but-no-bgp {
      permissions [ clear network reset trace view ];
      allow-commands "(request system software add)|(show route$)";
      deny-commands "show bgp";
    }
  }
}
```

1. Create the **operator-and-boot** custom login class, give it **operator** level permission flags, and authorize it to use the **request system reboot** command.

```
[edit system login]
user@router# set class operator-and-boot permissions clear network reset trace view
user@router# set class operator-and-boot allow-commands request system reboot
```

2. Create the **operator-no-set** custom login class, give it **operator** level permission flags, and deny it access to the **set** command.

```
[edit system login]
user@router# set class operator-no-set clear network reset trace view
user@router# set class operator-no-set deny-commands set
```

3. Create the **operator-and-install-but-no-bgp** custom login class, give it **operator** level permission flags, authorize it to use the **request system software add** and **show route** commands, and deny it access to the **show bgp** command.

```
[edit system login]
user@router# set class operator-and-install-but-no-bgp clear network reset trace
view
user@router# set class operator-and-install-but-no-bgp request system software
add show route
user@router# set class operator-and-install-but-no-bgp show bgp
```

4. Check your configuration by using the **show system login** command.

```
user@router# show system login
class operator-and-boot {
  permissions [ clear network reset trace view ];
  allow-commands "request system reboot";
}
class operator-no-set {
  permissions [ clear network reset trace view ];
  deny-commands "set";
}
class operator-and-install-but-no-bgp {
  permissions [ clear network reset trace view ];
  allow-commands "(request system software add)|(show route$)";
  deny-commands "show bgp";
}
```

Related Documentation • [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)

Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements let you explicitly allow or deny users access privileges to portions of the configuration hierarchy. Each of these statements is added to named login classes and configured with one or more regular expressions to be allowed or denied. Each login class is assigned to specific users or user IDs.

The search and match methods differ in the two forms of these statements. You must select which form to use within a login class—you cannot configure **allow-configuration** and **allow-configuration-regexps** together in the same login class. You must select just one. If you have existing configurations using the **allow/deny-configuration** form of the statements, using the same configuration options with the **allow/deny-configuration-regexps** form of the statements might not produce the same results.

- **Allow/deny-configuration** statements perform slower matching, with more flexibility, especially in wildcard matching. However, it can take a very long time to evaluate all of the possible statements if a great number of full path regular expressions or wildcard expressions are configured, possibly impacting performance. These statements were introduced before Junos OS Release 7.4.

- **Allow/deny-configuration-regexps** statements perform faster matching, with less flexibility. You configure a set of strings in which each string is a regular expression, with spaces between the terms of the string. This provides very fast matching. However, it is more tedious to use wildcard expressions in this form of the statement, because you must set up wildcards for each token (term) of the space-delimited string you want to match. These statements were introduced in Junos OS Release 11.2.

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Example: Configuring User Permissions with Access Privilege Levels on page 830](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)

Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements

This example shows how to set up configuration access privileges using the **allow-configuration-regexps** and **deny-configuration-regexps** statements.

- [Requirements on page 835](#)
- [Overview on page 835](#)
- [Configuration on page 836](#)
- [Examples Using Allow or Deny Configurations with Regular Expressions on page 836](#)

Requirements

This example uses the following hardware and software components:

- One Juniper Networks M Series, MX Series, or T Series device
- Junos OS Release 11.2 or later
 - There must be at least one user assigned to a login class.
 - There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

The **allow-configuration-regexps** and **deny-configuration-regexps** statements let you explicitly allow or deny users assigned to named user classes access privileges to portions of the configuration hierarchy, giving the system administrator precision control over who can change specific configurations in the system.



NOTE: The statements **allow-configuration-regexps** and **deny-configuration-regexps** perform similar functions as the statements **allow-configuration** and **deny-configuration**, except you can configure sets of strings in which the strings include spaces when using the first set of statements. You cannot use the two kinds of statements together.

Configuration

To set up configuration access privileges:

1. To explicitly allow one or more individual configuration mode hierarchies that would otherwise be denied, include the **allow-configuration-regexps** statement at the **[edit system login class class-name]** hierarchy level, configured with the regular expressions to be allowed.

```
[edit system login class class-name]
user@host# set allow-configuration-regexps "regular expression 1" "regular expression
2" "regular expression 3" "regular expression 4" ...
```

2. To explicitly deny one or more individual configuration hierarchies that would otherwise be allowed, include the **deny-configuration-regexps** statement at the **[edit system login class class-name]** hierarchy level, configured with the regular expressions to be denied.

```
[edit system login class class-name]
user@host# set deny-configuration-regexps "regular expression 1" "regular-expression
2" "regular expression 3" "regular expression 4"...
```

3. Assign the login class to one or more users.

```
[edit system login]
user@host# set user username class class-name
```

4. Commit your changes.

Users assigned this login class have the permissions you have set for the class.

Examples Using Allow or Deny Configurations with Regular Expressions

Purpose This section provides examples of access privilege configurations to give you ideas for creating configurations appropriate for your system. You can use combinations of privilege statements for configuration access and for operational mode commands to give precise control over classes of access privileges.

Allow Configuration Changes The following example login class lets the user make changes at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to the permissions specified by the **configure** permissions flag, which allows the user to enter configuration mode using the **configure** command.

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "system services"
```

Deny Configuration Changes The following example login class lets the user perform all operations allowed by the **all** permissions flag. However, it denies modifying the configuration at the **[edit system services]** hierarchy level.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-configuration-regexps "system services"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@host# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m ."
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot edit the configuration or issue commands (such as **commit**) at the **[edit system login class]** or the **[edit system services]** hierarchy levels:

```
[edit system login class class-name]
user@host# set deny-configuration "system login class" "system services"
```

Allow and Deny Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to **[system "interfaces .*" unit .*" family inet address .*" protocols]**. However, the user is denied configuration access to the SNMP hierarchy level.



NOTE: You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use [*] or [.*] alone.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps system "interfaces .* unit .* family inet
address ." protocols
user@host# set deny-configuration-regexps snmp
```

Allow and Deny Multiple Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to multiple hierarchy levels for interfaces. It denies configuration access to the **[edit system]** and **[edit protocols]** hierarchy levels.



NOTE: You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps "interfaces .* description ." "interfaces .*
unit .* description ." "interfaces .* unit .* family inet address ." "interfaces .* disable"
user@host# set deny-configuration-regexps "system" "protocols"
```

Allow Configuration Changes and Deny Operations Commands

You can combine allow and deny configuration statements with allow and deny operational commands statements to fine-tune access privileges. The following example login class uses a combination of the **deny-commands** operational permissions statement and the **allow-configuration-regexps** configuration permissions statement to let the user configure and commit changes to the OSPF and BGP protocols. However, this class of user cannot issue the **show system statistics** or the **show bgp summary** commands.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-commands "(show system statistics)|(show bgp summary)"
user@host# set allow-configuration-regexps "protocols ospf|bgp"
```

The following shows permissions set for individual configuration mode hierarchies:

```
[edit]
system {
  login { # This login class has operator privileges and the additional ability to edit
    # configuration at the system services hierarchy level.
    class only-system-services {
      permissions [ configure ];
      allow-configuration "system services";
    }
    # services commands.
    class all-except-system-services { # This login class has operator privileges but
      # cannot edit any system services configuration.
      permissions [ all ];
      deny-configuration "system services";
    }
  }
}
```

Verification To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.
2. Assign the login class to a *username*.
3. Log in as the *username* assigned with the new login class.
4. Attempt to perform the configurations that have been allowed or denied.
 - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
 - You should not be able to perform configuration changes to hierarchy levels and regular expressions that have been denied.
 - Denied expressions should take precedence over allowed expressions.
 - Any allowed or denied expressions should take precedence over any permissions granted with the **permissions** statement.

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Example: Configuring User Permissions with Access Privilege Levels on page 830](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)

CHAPTER 42

Permissions Flags for User Access Privileges

- [Access Privilege User Permission Flags Overview on page 840](#)
- [access on page 841](#)
- [access-control on page 842](#)
- [admin on page 843](#)
- [admin-control on page 844](#)
- [all-control on page 844](#)
- [clear on page 845](#)
- [configure on page 895](#)
- [control on page 896](#)
- [field on page 896](#)
- [firewall on page 896](#)
- [firewall-control on page 897](#)
- [floppy on page 898](#)
- [flow-tap on page 898](#)
- [flow-tap-control on page 899](#)
- [flow-tap-operation on page 899](#)
- [idp-profiler-operation on page 899](#)
- [interface on page 900](#)
- [interface-control on page 901](#)
- [maintenance on page 901](#)
- [network on page 908](#)
- [pgcp-session-mirroring on page 910](#)
- [pgcp-session-mirroring-control on page 910](#)
- [reset on page 911](#)
- [rollback on page 912](#)
- [secret on page 912](#)

- [secret-control on page 913](#)
- [security on page 914](#)
- [security-control on page 918](#)
- [shell on page 921](#)
- [snmp on page 921](#)
- [system on page 921](#)
- [system-control on page 924](#)
- [trace on page 925](#)
- [trace-control on page 930](#)
- [view on page 935](#)
- [view-configuration on page 1008](#)

Access Privilege User Permission Flags Overview

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag.

For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

The permission flags listed in "Related Documentation" grant a specific set of access privileges. Each permission flag is listed with the operational mode commands and configuration hierarchy levels and statements for which that flag grants access.



NOTE: Each command listed represents that command and all subcommands with that command as a prefix. Each configuration statement listed represents the top of the configuration hierarchy to which that flag grants access.

Related Documentation

- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [access on page 841](#)
- [access-control on page 842](#)
- [admin on page 843](#)
- [admin-control on page 844](#)
- [all-control on page 844](#)

- [clear on page 845](#)
- [configure on page 895](#)
- [control on page 896](#)
- [field on page 896](#)
- [firewall on page 896](#)
- [firewall-control on page 897](#)
- [floppy on page 898](#)
- [flow-tap on page 898](#)
- [flow-tap-operation on page 899](#)
- [idp-profiler-operation on page 899](#)
- [interface on page 900](#)
- [interface-control on page 901](#)
- [maintenance on page 901](#)
- [network on page 908](#)
- [pgcp-session-mirroring on page 910](#)
- [pgcp-session-mirroring-control on page 910](#)
- [reset on page 911](#)
- [rollback on page 912](#)
- [secret on page 912](#)
- [secret-control on page 913](#)
- [security on page 914](#)
- [security-control on page 918](#)
- [shell on page 921](#)
- [snmp on page 921](#)
- [system on page 921](#)
- [system-control on page 924](#)
- [trace on page 925](#)
- [trace-control on page 930](#)
- [view on page 935](#)
- [view-configuration on page 1008](#)

access

Can view the access configuration in configuration mode.

Commands No associated CLI commands.

**Configuration
Hierarchy Levels**

```
[edit access]
[edit access diameter]
[edit access ppp-options]
[edit access radius]
[edit dynamic-profile]
[edit logical-systems access]
[edit logical-systems routing-instances instance system services
static-subscribers access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
dynamic-profile]
[edit routing-instances instance system services static-subscribers group
access-profile]
[edit routing-instances instance system services static-subscribers group
dynamic-profile]
[edit system services extensible-subscriber-services access-profile]
[edit system services static-subscribers access-profile]
[edit system services static-subscribers dynamic-profile]
[edit system services static-subscribers group access-profile]
[edit system services static-subscribers group dynamic-profile]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [access-control on page 842](#)

access-control

Can view access configuration information. Can edit access configuration at the **[edit access]**, **[edit logical-systems]**, **[edit routing-instances]**, and **[edit system services]** hierarchy levels.

**Configuration
Hierarchy Levels**

```
[edit access]
[edit access ppp-options]
[edit dynamic-profile]
[edit logical-systems access]
```

```
[edit logical-systems routing-instances instance system services
static-subscribers access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
dynamic-profile]
[edit routing-instances instance system services static-subscribers group
access-profile]
[edit routing-instances instance system services static-subscribers group
dynamic-profile]
[edit system services static-subscribers access-profile]
[edit system services static-subscribers dynamic-profile]
[edit system services static-subscribers group access-profile]
[edit system services static-subscribers group dynamic-profile]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [access on page 841](#)

admin

Can view user account information in configuration mode.

Commands	show system audit
Configuration Hierarchy Levels	<pre>[edit protocols uplink-failure-detection] [edit system] [edit system accounting] [edit system diag-port-authentication] [edit system extensions] [edit system login] [edit system pic-console-authentication] [edit system root-authentication] [edit system services ssh ciphers] [edit system services ssh client-alive-count-max] [edit system services ssh client-alive-interval]] [edit system services ssh hostkey-algorithm] [edit system services ssh key-exchange] [edit system services ssh macs] [edit system services ssh max-sessions-per-connection]</pre>

```
[edit system services ssh no-tcp-fowarding]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
[edit system services ssh tcp-fowarding]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [admin-control on page 844](#)

admin-control

Can view user account information and configure it at the **[edit system]** hierarchy level.

Commands

```
show system audit
```

**Configuration
Hierarchy Levels**

```
[edit protocols uplink-failure-detection]
[edit system]
[edit system accounting]
[edit system diag-port-authentication]
[edit system extensions]
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh ciphers]
[edit system services ssh hostkey-algorithm]
[edit system services ssh key-exchange]
[edit system services ssh macs]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [admin on page 843](#)

all-control

Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.

Commands	All CLI commands.
Configuration Hierarchy Levels	All CLI configuration hierarchy levels and statements.
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 830 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834

clear

Can clear (delete) information learned from the network that is stored in various network databases.

Commands	<pre> clear clear amt clear amt statistics <clear-amt-statistics> clear amt tunnel clear-amt-tunnel clear amt tunnel gateway-address <clear amt tunnel gateway-address> clear amt tunnel statistics <clear-amt-tunnel-statistics> clear amt tunnel statistics gateway-address <clear-amt-tunnel-gateway-address-statistics> clear amt tunnel statistics tunnel-interface <clear-amt-tunnel-interface-statistics> clear amt tunnel tunnel-interface <clear-amt-tunnel-interface> clear ancp clear ancp neighbor <clear-ancp-neighbor-connection> clear ancp statistics <clear-ancp-statistics> clear ancp subscriber <clear-ancp-subscriber-connection> clear-appqos-counter clear-appqos-rate-limiter-statistics clear-appqos-rule-statistics clear arp <clear-arp-table> clear auto-configuration clear auto-configuration interfaces <clear-auto-configuration-interfaces> clear bfd clear bfd adaptation <clear-bfd-adaptation-information> clear bfd adaptation address <clear-bfd-adaptation-address> clear bfd adaptation discriminator <clear-bfd-adaptation-discriminator> clear bfd session </pre>
-----------------	---

```
<clear-bfd-session-information>
clear bfd session address
<clear-bfd-session-address>
clear bfd session discriminator
<clear-bfd-session-discriminator>
clear bgp
clear bgp damping
  <clear-bgp-damping>
clear bgp neighbor
  <clear-bgp-neighbor>
clear bgp table
  <clear-bgp-table>
clear bridge
clear bridge evpn
clear bridge evpn arp-table
<clear-bridge-evpn-arp-table>
clear bridge mac-table
  <clear-bridge-mac-table>
clear bridge mac-table interface
  <clear-bridge-interface-mac-table>
clear bridge recovery-timeout
<clear-bridge-recovery>
clear bridge recovery-timeout interface
<clear-bridge-recovery-interface>
clear captive-portal
clear captive-portal firewall
<clear-captive-portal-firewall>
clear captive-portal firewall interface
<clear-captive-portal-firewall-interface>
clear captive-portal interface
<clear-captive-portal-interface-session>
clear captive-portal mac-address
<clear-captive-portal-mac-session>
clear cli
clear cli logical-system
<clear-cli-logical-system>
clear database-replication
clear database-replication statistics
  <clear-database-replication-statistics-information>
clear ddos-protection
clear ddos-protection protocols
clear ddos-protection protocols amtv4
clear ddos-protection protocols amtv4 aggregate
clear ddos-protection protocols amtv4 aggregate culprit-flows
clear ddos-protection protocols amtv4 aggregate states
clear ddos-protection protocols amtv4 aggregate statistics
clear ddos-protection protocols amtv4 culprit-flows
clear ddos-protection protocols amtv4 states
clear ddos-protection protocols amtv4 statistics
clear ddos-protection protocols amtv6
clear ddos-protection protocols amtv6 aggregate
clear ddos-protection protocols amtv6 aggregate culprit-flows
<clear-ddos-amtv6-aggregate-flows>
clear ddos-protection protocols amtv6 aggregate states
<clear-ddos-amtv6-aggregate-states>
clear ddos-protection protocols amtv6 aggregate statistics
<clear-ddos-amtv6-aggregate-statistics>
clear ddos-protection protocols amtv6 culprit-flows
<clear-ddos-amtv6-flows>
clear ddos-protection protocols amtv6 states
<clear-ddos-amtv6-states>
```

```
clear ddos-protection protocols amtv6 statistics
<clear-ddos-amtv6-statistics>
clear ddos-protection protocols ancp aggregate culprit-flows
<clear-ddos-ancp-aggregate-flows>
clear ddos-protection protocols ancp culprit-flows
clear ddos-protection protocols ancp
clear ddos-protection protocols ancp aggregate
clear ddos-protection protocols ancp aggregate states
clear ddos-protection protocols ancp aggregate statistics
<clear-ddos-ancp-aggregate-statistics>
clear ddos-protection protocols ancp states
<clear-ddos-ancp-states>
clear ddos-protection protocols ancp statistics
<clear-ddos-ancp-statistics>
clear ddos-protection protocols ancpv6
clear ddos-protection protocols ancpv6 aggregate
clear ddos-protection protocols ancpv6 aggregate states

clear ddos-protection protocols ancpv6 aggregate culprit-flows
clear ddos-protection protocols arp aggregate statistics
clear-ddos-arp-aggregate-statistics
clear ddos-protection protocols arp aggregate culprit-flows
clear ddos-protection protocols arp states
clear-ddos-arp-states
clear ddos-protection protocols arp statistics
<clear-ddos-arp-statistics>
clear ddos-protection protocols arp culprit-flows
clear ddos-protection protocols atm
clear ddos-protection protocols atm aggregate
clear ddos-protection protocols atm aggregate culprit-flows
clear ddos-protection protocols atm aggregate states
<clear-ddos-atm-aggregate-states>
clear ddos-protection protocols atm aggregate statistics
<clear-ddos-atm-aggregate-statistics>
clear ddos-protection protocols atm culprit-flows
clear ddos-protection protocols bfd aggregate culprit-flows
clear ddos-protection protocols atm states
clear-ddos-atm-states
clear ddos-protection protocols atm statistics
clear-ddos-atm-statistics
clear ddos-protection protocols bfd
clear ddos-protection protocols bfd aggregate
clear ddos-protection protocols bfd culprit-flows
clear ddos-protection protocols bfd aggregate states
clear-ddos-bfd-aggregate-states
  clear ddos-protection protocols bfd aggregate statistics
clear-ddos-bfd-aggregate-statistics
  clear ddos-protection protocols bfd states
clear-ddos-bfd-states
clear ddos-protection protocols bfd statistics
clear-ddos-bfd-statistics
clear ddos-protection protocols bfdv6
clear ddos-protection protocols bfdv6 aggregate
clear ddos-protection protocols bfdv6 culprit-flows
clear ddos-protection protocols bfdv6 aggregate states
clear-ddos-bfdv6-aggregate-states
clear ddos-protection protocols bfdv6 aggregate statistics
clear-ddos-bfdv6-aggregate-statistics
clear ddos-protection protocols bfdv6 states
clear-ddos-bfdv6-states
clear ddos-protection protocols bfdv6 statistics
```

```
clear-ddos-bfdv6-statistics
clear ddos-protection protocols bgp
clear ddos-protection protocols bgp aggregate
clear ddos-protection protocols bgp aggregate culprit-flows
clear ddos-protection protocols bgp aggregate states
clear-ddos-bgp-aggregate-states
clear ddos-protection protocols bgp aggregate statistics
clear ddos-protection protocols bgp culprit-flows
clear ddos-protection protocols bgp states
clear-ddos-bgp-states
clear ddos-protection protocols bgp statistics
clear-ddos-bgp-statistics
clear ddos-protection protocols bgpv6
clear ddos-protection protocols bgpv6 aggregate
clear ddos-protection protocols bgpv6 aggregate culprit-flows
clear ddos-protection protocols bgpv6 aggregate states
clear-ddos-bgpv6-aggregate-states
clear ddos-protection protocols bgpv6 aggregate statistics
clear-ddos-bgpv6-aggregate-statistics
clear ddos-protection protocols bgpv6 states
clear-ddos-bgp-aggregate-states
clear-ddos-bgp-aggregate-statistics
clear-ddos-bgp-states
clear-ddos-bgp-statistics
clear-ddos-bgpv6-aggregate-states
clear-ddos-bgpv6-aggregate-statistics
clear-ddos-bgpv6-states
clear ddos-protection protocols bgpv6 statistics
<clear-ddos-bgpv6-statistics>
clear ddos-protection protocols culprit-flows
clear ddos-protection protocols demux-autosense
clear ddos-protection protocols demux-autosense aggregate
clear ddos-protection protocols demux-autosense aggregate culprit-flows
clear ddos-protection protocols demux-autosense aggregate states
clear-ddos-demuxauto-aggregate-states
clear ddos-protection protocols demux-autosense aggregate statistics
clear ddos-protection protocols demux-autosense culprit-flows
clear ddos-protection protocols demux-autosense states
clear-ddos-demuxauto-states
clear ddos-protection protocols demux-autosense statistics
clear-ddos-demuxauto-statistics
clear ddos-protection protocols dhcpv4
clear ddos-protection protocols dhcpv4 ack
clear ddos-protection protocols dhcpv4 ack culprit-flows
clear ddos-protection protocols dhcpv4 ack states
clear ddos-protection protocols dhcpv4 ack statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4v6
clear ddos-protection protocols dhcpv4v6 aggregate
clear ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<clear-ddos-dhcpv4v6-aggregate-flows>
clear ddos-protection protocols dhcpv4v6 aggregate states
<clear-ddos-dhcpv4v6-aggregate-states>
clear ddos-protection protocols dhcpv4v6 aggregate statistics
<clear-ddos-dhcpv4v6-aggregate-statistics>
clear ddos-protection protocols dhcpv4v6 culprit-flows
<clear-ddos-dhcpv4v6-flows>
clear ddos-protection protocols dhcpv4v6 states
<clear-ddos-dhcpv4v6-states>
clear ddos-protection protocols dhcpv4v6 statistics
<clear-ddos-dhcpv4v6-statistics>
```



```
clear-ddos-demuxauto-aggregate-states
clear-ddos-demuxauto-aggregate-statistics
clear-ddos-demuxauto-states
clear-ddos-demuxauto-statistics
clear-ddos-dhcpv4-ack-states
clear ddos-protection protocols dhcpv4 ack statistics
clear-ddos-dhcpv4-ack-statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4 aggregate states
clear-ddos-dhcpv4-aggregate-states
clear ddos-protection protocols dhcpv4 aggregate statistics
clear-ddos-dhcpv4-aggregate-statistics
clear ddos-protection protocols dhcpv4 bad-packets
clear ddos-protection protocols dhcpv4 bad-packets states
clear-ddos-dhcpv4-bad-pack-states
clear ddos-protection protocols dhcpv4 bad-packets statistics
clear-ddos-dhcpv4-bad-pack-statistics
clear ddos-protection protocols dhcpv4 bootp
clear ddos-protection protocols dhcpv4 bootp states
clear-ddos-dhcpv4-bootp-states
clear ddos-protection protocols dhcpv4 bootp statistics
clear-ddos-dhcpv4-bootp-statistics
clear ddos-protection protocols dhcpv4 decline
clear ddos-protection protocols dhcpv4 decline culprit-flows
clear ddos-protection protocols dhcpv4 decline states
clear-ddos-dhcpv4-decline-states
clear ddos-protection protocols dhcpv4 decline statistics
clear-ddos-dhcpv4-decline-statistics
clear ddos-protection protocols dhcpv4 discover
clear ddos-protection protocols dhcpv4 discover states
clear-ddos-dhcpv4-discover-states
clear ddos-protection protocols dhcpv4 discover statistics
clear-ddos-dhcpv4-discover-statistics
clear ddos-protection protocols dhcpv4 force-renew
clear ddos-protection protocols dhcpv4 force-renew culprit-flows
clear ddos-protection protocols dhcpv4 force-renew states
clear-ddos-dhcpv4-forcerenew-states
clear ddos-protection protocols dhcpv4 force-renew statistics
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 inform
clear ddos-protection protocols dhcpv4 inform culprit-flows
clear ddos-protection protocols dhcpv4 inform states
clear-ddos-dhcpv4-decline-states
clear-ddos-dhcpv4-decline-statistics
clear-ddos-dhcpv4-discover-states
clear-ddos-dhcpv4-discover-statistics
clear-ddos-dhcpv4-forcerenew-states
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 unclassified culprit-flows
clear ddos-protection protocols dhcpv4 unclassified states
clear-ddos-dhcpv4-unclass-states
clear ddos-protection protocols dhcpv4 unclassified statistics
clear-ddos-dhcpv4-unclass-statistics
clear ddos-protection protocols dhcpv6
clear ddos-protection protocols dhcpv6 advertise
clear ddos-protection protocols dhcpv6 advertise culprit-flows
clear ddos-protection protocols dhcpv6 advertise states
clear-ddos-dhcpv6-advertise-states
clear ddos-protection protocols dhcpv6 advertise statistics
clear-ddos-dhcpv6-advertise-statistics
clear ddos-protection protocols dhcpv6 aggregate
```

```
clear ddos-protection protocols dhcpv6 aggregate states
clear-ddos-dhcpv6-aggregate-states
clear ddos-protection protocols dhcpv6 aggregate statistics
clear-ddos-dhcpv6-aggregate-statistics
clear ddos-protection protocols dhcpv6 confirm
clear ddos-protection protocols dhcpv6 confirm culprit-flows
clear ddos-protection protocols dhcpv6 confirm states
clear-ddos-dhcpv6-confirm-states
clear ddos-protection protocols dhcpv6 confirm statistics
clear-ddos-dhcpv6-confirm-statistics
clear ddos-protection protocols dhcpv6 decline
clear ddos-protection protocols dhcpv6 decline states
clear-ddos-dhcpv6-decline-states
clear ddos-protection protocols dhcpv6 decline statistics
clear-ddos-dhcpv6-decline-statistics
clear ddos-protection protocols dhcpv6 information-request
clear ddos-protection protocols dhcpv6 information-request states
clear-ddos-dhcpv6-info-req-states
clear ddos-protection protocols dhcpv6 information-request statistics
clear-ddos-dhcpv6-info-req-statistics
clear ddos-protection protocols dhcpv6 leasequery
clear ddos-protection protocols dhcpv6 leasequery states
clear-ddos-dhcpv6-leasequery-states
clear ddos-protection protocols dhcpv6 leasequery statistics
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-data
clear ddos-protection protocols dhcpv6 leasequery-data states
clear ddos-protection protocols dhcpv6 leasequery-data statistics
clear ddos-protection protocols garp-reply
clear ddos-protection protocols garp-reply aggregate
clear ddos-protection protocols garp-reply aggregate culprit-flows
<clear-ddos-garp-reply-aggregate-flows>
clear ddos-protection protocols garp-reply aggregate states
<clear-ddos-garp-reply-aggregate-states>
clear ddos-protection protocols garp-reply aggregate statistics
<clear-ddos-garp-reply-aggregate-statistics>
clear ddos-protection protocols garp-reply culprit-flows
<clear-ddos-garp-reply-flows>
clear ddos-protection protocols garp-reply states
<clear-ddos-garp-reply-states>
clear ddos-protection protocols garp-reply statistics
<clear-ddos-garp-reply-statistics>
clear ddos-protection protocols gre hbc
clear ddos-protection protocols gre hbc culprit-flows
<clear-ddos-gre-hbc-flows>
clear ddos-protection protocols gre hbc states
<clear-ddos-gre-hbc-states>
clear ddos-protection protocols gre hbc statistics
<clear-ddos-gre-hbc-statistics>
clear ddos-protection protocols gre punt
clear ddos-protection protocols gre punt culprit-flows
<clear-ddos-gre-punt-flows>
clear ddos-protection protocols gre punt states
<clear-ddos-gre-punt-states>
clear ddos-protection protocols gre punt statistics
<clear-ddos-gre-punt-statistics>
clear ddos-protection protocols ipmc-reserved
clear ddos-protection protocols ipmc-reserved aggregate
clear ddos-protection protocols ipmc-reserved aggregate culprit-flows
<clear-ddos-ipmc-reserved-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate states
```

```

<clear-ddos-ipmc-reserved-aggregate-states>
clear ddos-protection protocols ipmc-reserved aggregate statistics
<clear-ddos-ipmc-reserved-aggregate-statistics>
clear ddos-protection protocols ipmc-reserved culprit-flows
<clear-ddos-ipmc-reserved-flows>
clear ddos-protection protocols ipmc-reserved states
<clear-ddos-ipmc-reserved-states>
clear ddos-protection protocols ipmc-reserved statistics
<clear-ddos-ipmc-reserved-statistics>
clear ddos-protection protocols ipmcast-miss
clear ddos-protection protocols ipmcast-miss aggregate
clear ddos-protection protocols ipmcast-miss aggregate culprit-flows
<clear-ddos-ipmcast-miss-aggregate-flows>
clear ddos-protection protocols ipmcast-miss aggregate states
<clear-ddos-ipmcast-miss-aggregate-states>
clear ddos-protection protocols ipmcast-miss aggregate statistics
<clear-ddos-ipmcast-miss-aggregate-statistics>
clear ddos-protection protocols ipmcast-miss culprit-flows
<clear-ddos-ipmcast-miss-flows>
clear ddos-protection protocols ipmcast-miss states
<clear-ddos-ipmcast-miss-states>
clear ddos-protection protocols ipmcast-miss statistics
<clear-ddos-ipmcast-miss-statistics>
clear ddos-protection protocols l3dest-miss
clear ddos-protection protocols l3dest-miss aggregate
clear ddos-protection protocols l3dest-miss aggregate culprit-flows
<clear-ddos-l3dest-miss-aggregate-flows>
clear ddos-protection protocols l3dest-miss aggregate states
<clear-ddos-l3dest-miss-aggregate-states>
clear ddos-protection protocols l3dest-miss aggregate statistics
<clear-ddos-l3dest-miss-aggregate-statistics>
clear ddos-protection protocols l3dest-miss culprit-flows
<clear-ddos-l3dest-miss-flows>
clear ddos-protection protocols l3dest-miss states
<clear-ddos-l3dest-miss-states>
clear ddos-protection protocols l3dest-miss statistics
<clear-ddos-l3dest-miss-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-aggregate-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate states
<clear-ddos-l3mc-sgv-hit-icl-aggregate-states>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate statistics
<clear-ddos-l3mc-sgv-hit-icl-aggregate-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
clear ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl states
<clear-ddos-l3mc-sgv-hit-icl-states>
clear ddos-protection protocols l3mc-sgv-hit-icl statistics
<clear-ddos-l3mc-sgv-hit-icl-statistics>
clear ddos-protection protocols l3mtu-fail
clear ddos-protection protocols l3mtu-fail aggregate
clear ddos-protection protocols l3mtu-fail aggregate culprit-flows
<clear-ddos-l3mtu-fail-aggregate-flows>
clear ddos-protection protocols l3mtu-fail aggregate states
<clear-ddos-l3mtu-fail-aggregate-states>
clear ddos-protection protocols l3mtu-fail aggregate statistics
<clear-ddos-l3mtu-fail-aggregate-statistics>
clear ddos-protection protocols l3mtu-fail culprit-flows

```

```
<clear-ddos-l3mtu-fail-flows>
clear ddos-protection protocols l3mtu-fail states
<clear-ddos-l3mtu-fail-states>
clear ddos-protection protocols l3mtu-fail statistics
<clear-ddos-l3mtu-fail-statistics>
clear ddos-protection protocols l3nhop
clear ddos-protection protocols l3nhop aggregate
clear ddos-protection protocols l3nhop aggregate culprit-flows
<clear-ddos-l3nhop-aggregate-flows>
clear ddos-protection protocols l3nhop aggregate states
<clear-ddos-l3nhop-aggregate-states>
clear ddos-protection protocols l3nhop aggregate statistics
<clear-ddos-l3nhop-aggregate-statistics>
clear ddos-protection protocols l3nhop culprit-flows
<clear-ddos-l3nhop-flows>
clear ddos-protection protocols l3nhop states
<clear-ddos-l3nhop-states>
clear ddos-protection protocols l3nhop statistics
<clear-ddos-l3nhop-statistics>
clear ddos-protection protocols localnh
clear ddos-protection protocols localnh aggregate
clear ddos-protection protocols localnh aggregate culprit-flows
<clear-ddos-localnh-aggregate-flows>
clear ddos-protection protocols localnh aggregate states
<clear-ddos-localnh-aggregate-states>
clear ddos-protection protocols localnh aggregate statistics
<clear-ddos-localnh-aggregate-statistics>
clear ddos-protection protocols localnh culprit-flows
<clear-ddos-localnh-flows>
clear ddos-protection protocols localnh states
<clear-ddos-localnh-states>
clear ddos-protection protocols localnh statistics
<clear-ddos-localnh-statistics>
clear-ddos-dhcpv4-unclass-states
clear-ddos-dhcpv4-unclass-statistics
clear-ddos-dhcpv6-advertise-states
clear-ddos-dhcpv6-advertise-statistics
clear-ddos-dhcpv6-aggregate-states
clear-ddos-dhcpv6-aggregate-statistics
clear-ddos-dhcpv6-confirm-states
clear-ddos-dhcpv6-confirm-statistics
clear-ddos-dhcpv6-decline-states
clear-ddos-dhcpv6-decline-statistics
clear-ddos-dhcpv6-info-req-states
clear-ddos-dhcpv6-info-req-statistics
clear-ddos-dhcpv6-leaseq-da-states
clear-ddos-dhcpv6-leasequery-states
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-done
clear ddos-protection protocols dhcpv6 leasequery-done states
clear-ddos-dhcpv6-leaseq-do-states
clear ddos-protection protocols dhcpv6 leasequery-done statistics
clear-ddos-dhcpv6-leaseq-do-statistics
clear ddos-protection protocols dhcpv6 leasequery-reply
clear ddos-protection protocols dhcpv6 leasequery-reply states
clear-ddos-dhcpv6-leaseq-re-states
clear ddos-protection protocols dhcpv6 leasequery-reply statistics
clear-ddos-dhcpv6-leaseq-re-statistics
clear ddos-protection protocols dhcpv6 rebind
clear ddos-protection protocols dhcpv6 rebind states
clear-ddos-dhcpv6-rebind-states
```

```
clear ddos-protection protocols dhcpv6 rebind statistics
clear-ddos-dhcpv6-rebind-statistics
clear ddos-protection protocols dhcpv6 reconfigure
clear ddos-protection protocols dhcpv6 reconfigure states
clear-ddos-dhcpv6-reconfig-states
clear ddos-protection protocols dhcpv6 reconfigure statistics
clear-ddos-dhcpv6-reconfig-statistics
clear ddos-protection protocols dhcpv6 relay-forward
clear ddos-protection protocols dhcpv6 relay-forward states
clear-ddos-dhcpv6-relay-for-states
clear ddos-protection protocols dhcpv6 relay-forward statistics
clear-ddos-dhcpv6-relay-for-statistics
clear ddos-protection protocols dhcpv6 relay-reply
clear ddos-protection protocols dhcpv6 relay-reply states
clear-ddos-dhcpv6-relay-rep-states
clear ddos-protection protocols dhcpv6 relay-reply statistics
clear-ddos-dhcpv6-relay-rep-statistics
clear ddos-protection protocols dhcpv6 release
clear ddos-protection protocols dhcpv6 release states
clear-ddos-dhcpv6-release-states
clear ddos-protection protocols dhcpv6 release statistics
clear-ddos-dhcpv6-release-statistics
clear ddos-protection protocols dhcpv6 renew
clear ddos-protection protocols dhcpv6 renew states
clear-ddos-dhcpv6-renew-states
clear ddos-protection protocols dhcpv6 renew statistics
clear-ddos-dhcpv6-renew-statistics
clear ddos-protection protocols dhcpv6 reply
clear ddos-protection protocols dhcpv6 reply states
clear-ddos-dhcpv6-reply-states
clear ddos-protection protocols dhcpv6 reply statistics
clear-ddos-dhcpv6-reply-statistics
clear ddos-protection protocols dhcpv6 request
clear ddos-protection protocols dhcpv6 request culprit-flows
clear ddos-protection protocols dhcpv6 request states
clear-ddos-dhcpv6-request-states
clear ddos-protection protocols dhcpv6 request statistics
clear-ddos-dhcpv6-request-statistics
clear ddos-protection protocols dhcpv6 solicit
clear ddos-protection protocols dhcpv6 solicit culprit-flows
clear ddos-protection protocols dhcpv6 solicit states
clear-ddos-dhcpv6-solicit-states
clear ddos-protection protocols dhcpv6 solicit statistics
clear-ddos-dhcpv6-solicit-statistics
clear ddos-protection protocols dhcpv6 states
clear-ddos-dhcpv6-states
clear ddos-protection protocols dhcpv6 statistics
clear-ddos-dhcpv6-statistics
clear ddos-protection protocols dhcpv6 unclassified
clear ddos-protection protocols dhcpv6 unclassified culprit-flows
clear ddos-protection protocols dhcpv6 unclassified states
clear-ddos-dhcpv6-unclass-states
clear ddos-protection protocols dhcpv6 unclassified statistics
clear-ddos-dhcpv6-unclass-statistics
clear ddos-protection protocols diameter
clear ddos-protection protocols diameter aggregate
clear ddos-protection protocols diameter aggregate culprit-flows
clear ddos-protection protocols diameter aggregate states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-dhcpv6-leaseq-da-statistics
clear-ddos-dhcpv6-leaseq-do-states
```

```
clear-ddos-dhcpv6-leaseq-do-statistics
clear-ddos-dhcpv6-leaseq-re-states
clear-ddos-dhcpv6-leaseq-re-statistics
clear-ddos-dhcpv6-rebind-states
clear-ddos-dhcpv6-rebind-statistics
clear-ddos-dhcpv6-reconfig-states
clear-ddos-dhcpv6-reconfig-statistics
clear-ddos-dhcpv6-relay-for-states
clear-ddos-dhcpv6-relay-for-statistics
clear-ddos-dhcpv6-relay-rep-states
clear-ddos-dhcpv6-relay-rep-statistics
clear-ddos-dhcpv6-release-states
clear-ddos-dhcpv6-release-statistics
clear-ddos-dhcpv6-renew-states
clear-ddos-dhcpv6-renew-statistics
clear-ddos-dhcpv6-reply-states
clear-ddos-dhcpv6-reply-statistics
clear-ddos-dhcpv6-request-states
clear-ddos-dhcpv6-request-statistics
clear-ddos-dhcpv6-solicit-states
clear-ddos-dhcpv6-solicit-statistics
clear-ddos-dhcpv6-states
clear-ddos-dhcpv6-statistics
clear-ddos-dhcpv6-unclass-states
clear-ddos-dhcpv6-unclass-statistics
clear-ddos-diameter-aggregate-states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-diameter-aggregate-statistics
clear ddos-protection protocols diameter states
clear-ddos-diameter-states
clear ddos-protection protocols diameter statistics
clear-ddos-diameter-statistics
clear ddos-protection protocols dns
clear ddos-protection protocols dns aggregate
clear ddos-protection protocols dns aggregate states
clear-ddos-dns-aggregate-states
clear ddos-protection protocols dns aggregate statistics
clear-ddos-dns-aggregate-statistics
clear ddos-protection protocols dns states
clear-ddos-dns-states
clear ddos-protection protocols dns statistics
clear-ddos-dns-statistics
clear ddos-protection protocols dtcp
clear ddos-protection protocols dtcp aggregate
clear ddos-protection protocols dtcp aggregate culprit-flows
clear ddos-protection protocols dtcp aggregate states
clear-ddos-dtcp-aggregate-states
clear ddos-protection protocols dtcp aggregate statistics
clear ddos-protection protocols dtcp culprit-flows
clear ddos-protection protocols dtcp states
clear-ddos-dtcp-states
clear ddos-protection protocols dtcp statistics
clear-ddos-dtcp-statistics
clear ddos-protection protocols dynamic-vlan
clear ddos-protection protocols dynamic-vlan aggregate
clear ddos-protection protocols dynamic-vlan aggregate culprit-flows
clear ddos-protection protocols dynamic-vlan aggregate states
clear-ddos-dynvlan-aggregate-states
clear ddos-protection protocols dynamic-vlan aggregate statistics
clear-ddos-dynvlan-aggregate-statistics
clear ddos-protection protocols dynamic-vlan states
```

```

clear-ddos-dynvlan-states
clear ddos-protection protocols dynamic-vlan statistics
clear-ddos-dynvlan-statistics
clear ddos-protection protocols egpv6
clear ddos-protection protocols egpv6 aggregate
clear ddos-protection protocols egpv6 aggregate culprit-flows
clear ddos-protection protocols egpv6 aggregate states
clear-ddos-egpv6-aggregate-states
clear ddos-protection protocols egpv6 aggregate statistics
clear-ddos-egpv6-aggregate-statistics
clear ddos-protection protocols egpv6 states
clear-ddos-egpv6-states
clear ddos-protection protocols egpv6 statistics
clear-ddos-egpv6-statistics
clear ddos-protection protocols eoam
clear ddos-protection protocols eoam aggregate
clear ddos-protection protocols eoam aggregate culprit-flows
clear ddos-protection protocols eoam aggregate states
clear-ddos-eoam-aggregate-states
clear ddos-protection protocols eoam aggregate statistics
clear-ddos-eoam-aggregate-statistics
clear ddos-protection protocols eoam states
clear-ddos-eoam-states
clear ddos-protection protocols eoam statistics
clear-ddos-eoam-statistics
clear ddos-protection protocols esmc
clear ddos-protection protocols esmc aggregate
clear ddos-protection protocols esmc aggregate culprit-flows
clear ddos-protection protocols esmc aggregate states
clear-ddos-esmc-aggregate-states
clear ddos-protection protocols esmc aggregate statistics
clear ddos-protection protocols esmc culprit-flows
clear ddos-protection protocols esmc states
clear-ddos-esmc-states
clear ddos-protection protocols esmc statistics
clear ddos-protection protocols fab-probe
clear ddos-protection protocols fab-probe aggregate
clear ddos-protection protocols fab-probe aggregate states
clear ddos-protection protocols fab-probe aggregate statistics
<clear-ddos-fab-probe-aggregate-statistics>
clear ddos-protection protocols martian-address
clear ddos-protection protocols martian-address aggregate
clear ddos-protection protocols martian-address aggregate culprit-flows
<clear-ddos-martian-address-aggregate-flows>
clear ddos-protection protocols martian-address aggregate states
<clear-ddos-martian-address-aggregate-states>
clear ddos-protection protocols martian-address aggregate statistics
<clear-ddos-martian-address-aggregate-statistics>
clear ddos-protection protocols martian-address culprit-flows
<clear-ddos-martian-address-flows>
clear ddos-protection protocols martian-address states
<clear-ddos-martian-address-states>
clear ddos-protection protocols martian-address statistics
<clear-ddos-martian-address-statistics>
clear-ddos-diameter-statistics
clear-ddos-dns-aggregate-states
clear-ddos-dns-aggregate-statistics
clear-ddos-dns-states
clear-ddos-dns-statistics
clear-ddos-dtcp-aggregate-states
clear-ddos-dtcp-aggregate-statistics

```

```
clear-ddos-dtcp-states
clear-ddos-dtcp-statistics
clear-ddos-dynvlan-aggregate-states
clear-ddos-dynvlan-aggregate-statistics
clear-ddos-dynvlan-states
clear-ddos-dynvlan-statistics
clear-ddos-egpv6-aggregate-states
clear-ddos-egpv6-aggregate-statistics
clear-ddos-egpv6-states
clear-ddos-egpv6-statistics
clear-ddos-eoam-aggregate-states
clear-ddos-eoam-aggregate-statistics
clear-ddos-eoam-states
clear-ddos-eoam-statistics
clear-ddos-esmc-aggregate-states
clear-ddos-esmc-aggregate-statistics
clear-ddos-esmc-states
clear ddos-protection protocols fab-probe states
<clear-ddos-fab-probe-states>
clear ddos-protection protocols fab-probe statistics
<clear-ddos-fab-probe-statistics>
clear-ddos-esmc-statistics
clear ddos-protection protocols firewall-host
clear ddos-protection protocols firewall-host aggregate
clear ddos-protection protocols firewall-host aggregate culprit-flows
clear ddos-protection protocols firewall-host aggregate states
clear-ddos-fw-host-aggregate-states
clear ddos-protection protocols firewall-host aggregate statistics
clear ddos-protection protocols firewall-host states
clear ddos-protection protocols firewall-host statistics
clear-ddos-esmc-statistics
clear-ddos-fw-host-aggregate-states
clear-ddos-fw-host-aggregate-statistics
<clear-ddos-fw-host-statistics>
clear-ddos-fw-host-states
clear ddos-protection protocols frame-relay
clear ddos-protection protocols frame-relay aggregate
clear ddos-protection protocols frame-relay aggregate culprit-flows
clear ddos-protection protocols frame-relay aggregate states
clear ddos-protection protocols frame-relay aggregate statistics
clear ddos-protection protocols frame-relay culprit-flows
clear ddos-protection protocols frame-relay frf15
clear ddos-protection protocols frame-relay frf15 culprit-flows
clear ddos-protection protocols frame-relay frf15 states
clear ddos-protection protocols frame-relay frf15 statistics
clear ddos-protection protocols frame-relay frf16
clear ddos-protection protocols frame-relay frf16 culprit-flows
clear ddos-protection protocols frame-relay frf16 states
clear ddos-protection protocols frame-relay frf16 statistics
clear ddos-protection protocols frame-relay states
clear ddos-protection protocols frame-relay statistics
clear ddos-protection protocols ftp
clear ddos-protection protocols ftp aggregate
clear ddos-protection protocols ftp aggregate culprit-flows
clear ddos-protection protocols ftp aggregate states
clear-ddos-ftp-aggregate-states
clear ddos-protection protocols ftp aggregate statistics
clear-ddos-ftp-aggregate-statistics
clear ddos-protection protocols ftp states
clear-ddos-ftp-states
clear ddos-protection protocols ftp statistics
```



```

clear-ddos-ftp-statistics
clear ddos-protection protocols ftpv6
clear ddos-protection protocols ftpv6 aggregate
clear ddos-protection protocols ftpv6 aggregate culprit-flows
clear ddos-protection protocols ftpv6 aggregate states
clear-ddos-ftp6-aggregate-states
clear ddos-protection protocols ftpv6 aggregate statistics
clear-ddos-ftp6-aggregate-statistics
clear ddos-protection protocols ftpv6 states
clear-ddos-ftp6-states
clear ddos-protection protocols ftpv6 statistics
clear-ddos-ftp6-statistics
clear ddos-protection protocols gre
clear ddos-protection protocols gre aggregate
clear ddos-protection protocols gre aggregate culprit-flow
clear ddos-protection protocols gre aggregate states
clear ddos-protection protocols gre culprit-flows
clear-ddos-ftp-statistics
clear-ddos-ftp6-aggregate-states
clear-ddos-ftp6-aggregate-statistics
clear-ddos-ftp6-states
clear-ddos-ftp6-statistics
clear-ddos-gre-aggregate-states
clear ddos-protection protocols gre aggregate statistics
clear-ddos-gre-aggregate-statistics
clear ddos-protection protocols gre states
clear-ddos-gre-states
clear ddos-protection protocols gre statistics
clear-ddos-gre-statistics
clear ddos-protection protocols icmp
clear ddos-protection protocols icmp aggregate
clear ddos-protection protocols icmp aggregate states
clear-ddos-icmp-aggregate-states
clear ddos-protection protocols icmp aggregate statistics
clear-ddos-icmp-aggregate-statistics
clear ddos-protection protocols icmp states
clear-ddos-icmp-states
clear ddos-protection protocols icmp statistics
clear-ddos-icmp-statistics
clear ddos-protection protocols icmpv6
clear ddos-protection protocols icmpv6 aggregate
clear ddos-protection protocols icmpv6 aggregate culprit-flows
clear ddos-protection protocols icmpv6 aggregate states
<clear-ddos-icmpv6-aggregate-states>
clear ddos-protection protocols icmpv6 aggregate statistics
<clear-ddos-icmp-aggregate-statistics>
<clear-ddos-icmpv6-aggregate-statistics>
clear ddos-protection protocols icmpv6 states
<clear-ddos-icmpv6-states>
clear ddos-protection protocols icmpv6 statistics
<clear-ddos-icmpv6-statistics>
clear ddos-protection protocols igmp
clear ddos-protection protocols igmp aggregate
clear ddos-protection protocols igmp aggregate culprit-flows
clear ddos-protection protocols igmp aggregate states
clear-ddos-igmp-aggregate-states
clear ddos-protection protocols igmp aggregate statistics
clear-ddos-igmp-aggregate-statistics
clear ddos-protection protocols igmp states
clear-ddos-igmp-states
clear ddos-protection protocols igmp statistics

```

```
clear-ddos-igmp-statistics
clear ddos-protection protocols igmp-snoop
clear ddos-protection protocols igmp-snoop aggregate
clear ddos-protection protocols igmp-snoop aggregate states
clear-ddos-igmp-snoop-aggregate-states
clear ddos-protection protocols igmp-snoop aggregate statistics
clear-ddos-igmp-snoop-aggregate-statistics
clear ddos-protection protocols igmp-snoop states
clear-ddos-igmp-snoop-states
clear ddos-protection protocols igmp-snoop statistics
clear-ddos-igmp-snoop-statistics
clear ddos-protection protocols igmpv4v6
clear ddos-protection protocols igmpv4v6 aggregate
clear ddos-protection protocols igmpv4v6 aggregate states
clear-ddos-igmpv4v6-aggregate-states
clear ddos-protection protocols igmpv4v6 aggregate statistics
clear ddos-protection protocols igmpv4v6 culprit-flows
clear ddos-protection protocols igmpv4v6 states
clear-ddos-igmpv4v6-states
clear ddos-protection protocols igmpv4v6 statistics
clear-ddos-igmpv4v6-statistics
clear ddos-protection protocols igmpv6
clear ddos-protection protocols igmpv6 aggregate
clear ddos-protection protocols igmpv6 aggregate culprit-flows
clear ddos-protection protocols igmpv6 aggregate states
clear ddos-protection protocols igmpv6 aggregate statistics
clear ddos-protection protocols igmpv6 states
clear ddos-protection protocols igmpv6 statistics
<clear-ddos-igmpv6-statistics>clear-ddos-igmp-snoop-states
clear-ddos-igmp-snoop-statistics
clear-ddos-igmp-statistics
clear-ddos-igmpv4v6-aggregate-states
clear-ddos-igmpv4v6-aggregate-statistics
clear-ddos-igmpv4v6-states
clear-ddos-igmpv4v6-statistics
clear-ddos-igmpv6-aggregate-states
clear ddos-protection protocols igmpv6 aggregate statistics
clear-ddos-igmpv6-aggregate-statistics
clear ddos-protection protocols igmpv6 states
clear-ddos-igmpv6-states
clear ddos-protection protocols inline-ka
clear ddos-protection protocols inline-ka aggregate
clear ddos-protection protocols inline-ka aggregate culprit-flows
clear ddos-protection protocols inline-ka aggregate states
clear ddos-protection protocols inline-ka aggregate statistics
clear ddos-protection protocols inline-ka culprit-flows
clear ddos-protection protocols inline-ka states
clear ddos-protection protocols inline-ka statistics
clear ddos-protection protocols inline-svcs
clear ddos-protection protocols inline-svcs aggregate
clear ddos-protection protocols inline-svcs aggregate culprit-flows
clear ddos-protection protocols inline-svcs aggregate states
clear ddos-protection protocols inline-svcs aggregate statistics
clear ddos-protection protocols inline-svcs culprit-flows
clear ddos-protection protocols inline-svcs states
clear ddos-protection protocols inline-svcs statistics
clear ddos-protection protocols ip-fragments
clear ddos-protection protocols ip-fragments aggregate
clear ddos-protection protocols ip-fragments aggregate states
clear-ddos-ip-frag-aggregate-states
clear ddos-protection protocols ip-fragments aggregate statistics
```

```

clear ddos-protection protocols ip-fragments culprit-flows
clear ddos-protection protocols ip-fragments first-fragment
clear ddos-protection protocols ip-fragments first-fragment states
clear-ddos-ip-frag-first-frag-states
clear ddos-protection protocols ip-fragments first-fragment statistics
clear-ddos-ip-frag-first-frag-statistics
clear ddos-protection protocols ip-fragments states
clear-ddos-ip-frag-states
clear ddos-protection protocols ip-fragments statistics
clear-ddos-ip-frag-statistics
clear ddos-protection protocols ip-fragments trail-fragment
clear ddos-protection protocols ip-fragments trail-fragment culprit-flows
clear ddos-protection protocols ip-fragments trail-fragment states
clear-ddos-ip-frag-trail-frag-states
clear ddos-protection protocols ip-fragments trail-fragment statistics
clear-ddos-ip-frag-trail-frag-statistics
clear ddos-protection protocols ip-options
clear ddos-protection protocols ip-options aggregate
clear ddos-protection protocols ip-options aggregate states
clear-ddos-ip-opt-aggregate-states
clear ddos-protection protocols ip-options aggregate statistics
clear-ddos-ip-opt-aggregate-statistics
clear ddos-protection protocols ip-options non-v4v6
clear ddos-protection protocols ip-options non-v4v6 states
<clear-ddos-ip-opt-non-v4v6-states>
clear-ddos-ip-frag-aggregate-states
clear-ddos-ip-frag-aggregate-statistics
clear-ddos-ip-frag-first-frag-states
clear-ddos-ip-frag-first-frag-statistics
clear-ddos-ip-frag-states
clear-ddos-ip-frag-statistics
clear-ddos-ip-frag-trail-frag-states
clear-ddos-ip-frag-trail-frag-statistics
clear-ddos-ip-opt-aggregate-states
clear-ddos-ip-opt-aggregate-statistics
clear ddos-protection protocols ip-options non-v4v6 statistics
<clear-ddos-ip-opt-non-v4v6-statistics>
clear ddos-protection protocols ip-options router-alert
clear ddos-protection protocols ip-options router-alert culprit-flows
clear ddos-protection protocols ip-options router-alert states
clear-ddos-ip-opt-rt-alert-states
clear ddos-protection protocols ip-options router-alert statistics
clear-ddos-ip-opt-rt-alert-statistics
clear ddos-protection protocols ip-options states
clear-ddos-ip-opt-states
clear ddos-protection protocols ip-options statistics
clear-ddos-ip-opt-statistics
clear ddos-protection protocols ip-options unclassified
clear ddos-protection protocols ip-options unclassified culprit-flows
clear ddos-protection protocols ip-options unclassified states
clear ddos-protection protocols ip-options unclassified statistics
clear-ddos-ip-opt-unclass-statistics
clear ddos-protection protocols ipv4-unclassified
clear ddos-protection protocols ipv4-unclassified aggregate
clear ddos-protection protocols ipv4-unclassified aggregate states
clear-ddos-ipv4-uncls-aggregate-states
clear ddos-protection protocols ipv4-unclassified aggregate statistics
clear-ddos-ipv4-uncls-aggregate-statistics
clear ddos-protection protocols ipv4-unclassified states
clear-ddos-ipv4-uncls-states
clear ddos-protection protocols ipv4-unclassified statistics

```

```
clear-ddos-ipv4-uncls-statistics
clear ddos-protection protocols ipv6-unclassified
clear ddos-protection protocols ipv6-unclassified aggregate
clear ddos-protection protocols ipv6-unclassified aggregate states
clear-ddos-ipv6-uncls-aggregate-states
clear ddos-protection protocols ipv6-unclassified aggregate statistics
clear-ddos-ipv6-uncls-aggregate-statistics
clear ddos-protection protocols ipv6-unclassified states
clear-ddos-ipv6-uncls-states
clear ddos-protection protocols ipv6-unclassified statistics
clear-ddos-ipv6-uncls-statistics
clear ddos-protection protocols isis
clear ddos-protection protocols isis aggregate
clear ddos-protection protocols isis aggregate culprit-flows
clear ddos-protection protocols isis aggregate states
clear-ddos-ip-opt-rt-alert-states
clear-ddos-ip-opt-rt-alert-statistics
clear-ddos-ip-opt-states
clear-ddos-ip-opt-statistics
clear-ddos-ip-opt-unclass-states
clear-ddos-ip-opt-unclass-statistics
clear-ddos-ipv4-uncls-aggregate-states
clear-ddos-isis-aggregate-states
clear ddos-protection protocols isis aggregate statistics
<clear-ddos-isis-aggregate-statistics>
clear ddos-protection protocols isis culprit-flows
clear ddos-protection protocols isis states
clear-ddos-isis-states
clear ddos-protection protocols isis statistics
clear-ddos-isis-statistics
clear ddos-protection protocols jfm
clear ddos-protection protocols jfm aggregate
clear ddos-protection protocols jfm aggregate culprit-flows
clear ddos-protection protocols jfm aggregate states
clear-ddos-jfm-aggregate-states
clear ddos-protection protocols jfm aggregate statistics
clear-ddos-jfm-aggregate-statistics
clear ddos-protection protocols jfm states
clear-ddos-jfm-states
clear ddos-protection protocols jfm statistics
<clear-ddos-jfm-statistics>
clear ddos-protection protocols keepalive
clear ddos-protection protocols keepalive aggregate
clear ddos-protection protocols keepalive aggregate culprit-flows
clear ddos-protection protocols keepalive aggregate states
clear ddos-protection protocols keepalive aggregate statistics
clear ddos-protection protocols keepalive culprit-flows
clear ddos-protection protocols keepalive states
clear ddos-protection protocols keepalive statistics
clear ddos-protection protocols l2pt
clear ddos-protection protocols l2pt aggregate
clear ddos-protection protocols l2pt aggregate states
clear ddos-protection protocols l2pt aggregate statistics
clear ddos-protection protocols l2pt culprit-flows
clear ddos-protection protocols l2pt states
clear ddos-protection protocols l2pt statistics
clear ddos-protection protocols l2tp
clear ddos-protection protocols l2tp aggregate
clear ddos-protection protocols l2tp aggregate culprit-flows
clear ddos-protection protocols l2tp aggregate states
clear-ddos-l2tp-aggregate-states
```

```
clear ddos-protection protocols l2tp aggregate statistics
clear-ddos-l2tp-aggregate-statistics
clear ddos-protection protocols l2tp states
clear-ddos-l2tp-states
clear ddos-protection protocols l2tp statistics
clear-ddos-l2tp-statistics
clear ddos-protection protocols lacp
clear ddos-protection protocols lacp aggregate
clear ddos-protection protocols lacp aggregate culprit-flows
clear ddos-protection protocols lacp aggregate states
clear-ddos-lacp-aggregate-states
clear ddos-protection protocols lacp aggregate statistics
clear-ddos-lacp-aggregate-statistics
clear ddos-protection protocols lacp states
clear-ddos-lacp-states
clear ddos-protection protocols lacp statistics
clear-ddos-lacp-statistics
clear ddos-protection protocols ldp
clear ddos-protection protocols ldp aggregate
clear ddos-protection protocols ldp aggregate culprit-flows
clear ddos-protection protocols ldp aggregate states
clear-ddos-isis-states
clear-ddos-isis-statistics
clear-ddos-jfm-aggregate-states
clear-ddos-jfm-aggregate-statistics
clear-ddos-jfm-states
clear-ddos-l2tp-aggregate-states
clear-ddos-l2tp-aggregate-statistics
clear-ddos-l2tp-states
clear-ddos-l2tp-statistics
clear-ddos-lacp-aggregate-states
clear-ddos-lacp-aggregate-statistics
clear-ddos-lacp-states
clear-ddos-lacp-statistics
clear-ddos-ldp-aggregate-states
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp statistics
clear ddos-protection protocols ldp statistics
clear-ddos-ldp-statistics
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate statistics
clear ddos-protection protocols ldpv6 aggregate statistics
clear-ddos-ldpv6-aggregate-statistics
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp
```

```
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp states
clear ddos-protection protocols lldp states
clear-ddos-lldp-states
clear ddos-protection protocols lldp statistics
clear ddos-protection protocols lldp statistics
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp states
clear ddos-protection protocols lmp states
clear ddos-protection protocols lmp statistics
clear ddos-protection protocols lmp statistics
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 culprit-flows
clear ddos-protection protocols lmpv6 states
clear-ddos-lmpv6-states
clear ddos-protection protocols lmpv6 statistics
clear-ddos-lmpv6-statistics
clear ddos-protection protocols mac-host
clear ddos-protection protocols mac-host aggregate
clear ddos-protection protocols mac-host aggregate culprit-flows
clear ddos-protection protocols mac-host aggregate states
clear-ddos-mac-host-aggregate-states
clear ddos-protection protocols mac-host aggregate statistics
clear-ddos-mac-host-aggregate-statistics
clear ddos-protection protocols mac-host states
clear-ddos-mac-host-states
clear ddos-protection protocols mac-host statistics
clear ddos-protection protocols mcast-snoop
clear ddos-protection protocols mcast-snoop aggregate
clear ddos-protection protocols mcast-snoop aggregate culprit-flows
clear ddos-protection protocols mcast-snoop aggregate states
clear ddos-protection protocols mcast-snoop aggregate statistics
clear ddos-protection protocols mcast-snoop culprit-flows
clear ddos-protection protocols mcast-snoop igmp
clear ddos-protection protocols mlp
clear ddos-protection protocols mlp add
```

```

clear ddos-protection protocols mlp add culprit-flows
<clear-ddos-mlp-add-flows>
clear ddos-protection protocols mlp add states
<clear-ddos-mlp-add-states>
clear ddos-protection protocols mlp add statistics
<clear-ddos-mlp-add-statistics>
clear ddos-protection protocols mlp aggregate
clear ddos-protection protocols mlp aggregate culprit-flows
clear ddos-protection protocols mlp aggregate states
clear-ddos-mlp-aggregate-states
clear ddos-protection protocols mlp aggregate statistics
clear-ddos-mlp-aggregate-statistics
clear ddos-protection protocols mlp aging-exception
clear ddos-protection protocols mlp aging-exception culprit-flows
clear ddos-protection protocols mlp aging-exception states
clear-ddos-mlp-aging-exc-states
clear ddos-protection protocols mlp aging-exception statistics
clear-ddos-mlp-aging-exc-statistics
clear ddos-protection protocols mlp packets
clear ddos-protection protocols mlp packets states
clear-ddos-mlp-packets-states
clear ddos-protection protocols mlp packets statistics
clear-ddos-mlp-packets-statistics
clear ddos-protection protocols mlp states
clear-ddos-mlp-states
clear ddos-protection protocols mlp statistics
clear-ddos-mlp-statistics
clear ddos-protection protocols mlp unclassified
clear ddos-protection protocols mlp unclassified states
clear-ddos-mlp-unclass-states
clear ddos-protection protocols mlp unclassified statistics
clear-ddos-mlp-unclass-statistics
clear ddos-protection protocols msdp
clear ddos-protection protocols msdp aggregate
clear ddos-protection protocols msdp aggregate states
clear-ddos-msdp-aggregate-states
clear ddos-protection protocols msdp aggregate statistics
clear ddos-protection protocols msdp culprit-flows
clear ddos-protection protocols msdp states
clear-ddos-msdp-states
clear ddos-protection protocols msdp statistics
clear-ddos-msdp-statistics
clear ddos-protection protocols msdpv6
clear ddos-protection protocols msdpv6 aggregate
clear ddos-protection protocols msdpv6 aggregate culprit-flows
clear ddos-protection protocols msdpv6 aggregate states
clear-ddos-msdpv6-aggregate-states
clear ddos-protection protocols msdpv6 aggregate statistics
clear-ddos-msdpv6-aggregate-statistics
clear ddos-protection protocols msdpv6 states
clear-ddos-msdpv6-states
clear ddos-protection protocols msdpv6 statistics
clear-ddos-msdpv6-statistics
clear ddos-protection protocols multicast-copy
clear ddos-protection protocols multicast-copy aggregate
clear ddos-protection protocols multicast-copy aggregate states
clear-ddos-mcast-copy-aggregate-states
clear ddos-protection protocols multicast-copy aggregate statistics
clear-ddos-mcast-copy-aggregate-statistics
clear ddos-protection protocols multicast-copy states
clear-ddos-mcast-copy-states

```

```
clear ddos-protection protocols multicast-copy statistics
clear-ddos-mcast-copy-statistics
clear ddos-protection protocols mvrp
clear ddos-protection protocols mvrp aggregate
clear ddos-protection protocols mvrp aggregate states
clear-ddos-mvrp-aggregate-states
clear ddos-protection protocols mvrp aggregate statistics
clear ddos-protection protocols mvrp culprit-flows
clear ddos-protection protocols mvrp states
clear-ddos-mvrp-states
clear ddos-protection protocols mvrp statistics
clear-ddos-mvrp-statistics
clear ddos-protection protocols ndpv6
clear ddos-protection protocols ndpv6 aggregate
clear ddos-protection protocols ndpv6 aggregate states
clear ddos-protection protocols ndpv6 aggregate statistics
clear ddos-protection protocols ndpv6 states
clear ddos-protection protocols ndpv6 statistics
clear ddos-protection protocols nonucast-switch
clear ddos-protection protocols nonucast-switch aggregate
clear ddos-protection protocols nonucast-switch aggregate culprit-flows
<clear-ddos-nonucast-switch-aggregate-flows>
clear ddos-protection protocols nonucast-switch aggregate states
<clear-ddos-nonucast-switch-aggregate-states>
clear ddos-protection protocols nonucast-switch aggregate statistics
<clear-ddos-nonucast-switch-aggregate-statistics>
clear ddos-protection protocols nonucast-switch culprit-flows
<clear-ddos-nonucast-switch-flows>
clear ddos-protection protocols nonucast-switch states
<clear-ddos-nonucast-switch-states>
clear ddos-protection protocols nonucast-switch statistics
<clear-ddos-nonucast-switch-statistics>
clear ddos-protection protocols ntp aggregate
clear ddos-protection protocols ntp aggregate states
clear-ddos-ntp-aggregate-states
clear ddos-protection protocols ntp aggregate statistics
clear ddos-protection protocols ntp culprit-flows
clear ddos-protection protocols ntp states
clear-ddos-ntp-states
clear ddos-protection protocols ntp statistics
clear-ddos-ntp-statistics
clear ddos-protection protocols oam-lfm
clear ddos-protection protocols oam-lfm aggregate
clear ddos-protection protocols oam-lfm aggregate states
clear-ddos-oam-lfm-aggregate-states
clear ddos-protection protocols oam-lfm aggregate statistics
clear-ddos-oam-lfm-aggregate-statistics
clear ddos-protection protocols oam-lfm states
clear-ddos-oam-lfm-states
clear ddos-protection protocols oam-lfm statistics
clear-ddos-oam-lfm-statistics
clear ddos-protection protocols ospf
clear ddos-protection protocols ospf aggregate
clear ddos-protection protocols ospf aggregate culprit-flows
clear ddos-protection protocols ospf aggregate states
clear-ddos-ospf-aggregate-states
clear ddos-protection protocols ospf aggregate statistics
clear-ddos-ospf-aggregate-statistics
clear ddos-protection protocols ospf states
clear ddos-protection protocols ospf statistics
clear ddos-protection protocols ospf-hello
```



```

clear ddos-protection protocols ospf-hello aggregate
clear ddos-protection protocols ospf-hello aggregate culprit-flows
<clear-ddos-ospf-hello-aggregate-flows>
clear ddos-protection protocols ospf-hello aggregate states
<clear-ddos-ospf-hello-aggregate-states>
clear ddos-protection protocols ospf-hello aggregate statistics
<clear-ddos-ospf-hello-aggregate-statistics>
clear ddos-protection protocols ospf-hello culprit-flows
<clear-ddos-ospf-hello-flows>
clear ddos-protection protocols ospf-hello states
<clear-ddos-ospf-hello-states>
clear ddos-protection protocols ospf-hello statistics
<clear-ddos-ospf-hello-statistics>
clear ddos-protection protocols ospfv3v6
clear ddos-protection protocols ospfv3v6 aggregate
clear ddos-protection protocols ospfv3v6 aggregate culprit-flows
clear ddos-protection protocols ospfv3v6 aggregate states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear ddos-protection protocols ospfv3v6 states
clear ddos-protection protocols ospfv3v6 statistics
clear-ddos-ldp-states
clear-ddos-ldp-states
clear-ddos-ldp-statistics
clear-ddos-ldp-statistics
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-states
clear-ddos-ldpv6-states
clear-ddos-ldpv6-statistics
clear-ddos-ldpv6-statistics
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-states
clear-ddos-lldp-states
clear-ddos-lldp-statistics
clear-ddos-lldp-statistics
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-states
clear-ddos-lmp-states
clear-ddos-lmp-statistics
clear-ddos-lmp-statistics
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-states
clear-ddos-lmpv6-statistics
clear-ddos-mac-host-aggregate-states
clear-ddos-mac-host-aggregate-statistics
clear-ddos-mac-host-states
clear-ddos-mac-host-statistics
clear-ddos-mcast-copy-aggregate-states
clear-ddos-mcast-copy-aggregate-statistics
clear-ddos-mcast-copy-states
clear-ddos-mcast-copy-statistics
clear-ddos-mlp-aggregate-states

```

```
clear-ddos-mlp-aggregate-statistics
clear-ddos-mlp-aging-exc-states
clear-ddos-mlp-aging-exc-statistics
clear-ddos-mlp-packets-states
clear-ddos-mlp-packets-statistics
clear-ddos-mlp-states
clear-ddos-mlp-statistics
clear-ddos-mlp-unclass-states
clear-ddos-mlp-unclass-statistics
clear-ddos-msdp-aggregate-states
clear-ddos-msdp-aggregate-statistics
clear-ddos-msdp-states
clear-ddos-msdp-statistics
clear-ddos-msdpv6-aggregate-states
clear-ddos-msdpv6-aggregate-statistics
clear-ddos-msdpv6-states
clear-ddos-msdpv6-statistics
clear-ddos-mvrp-aggregate-states
clear-ddos-mvrp-aggregate-statistics
clear-ddos-mvrp-states
clear-ddos-mvrp-statistics
clear-ddos-ntp-aggregate-states
clear-ddos-ntp-aggregate-statistics
clear-ddos-ntp-states
clear-ddos-ntp-statistics
clear-ddos-oam-lfm-aggregate-states
clear-ddos-oam-lfm-aggregate-statistics
clear-ddos-oam-lfm-states
clear-ddos-oam-lfm-statistics
clear-ddos-ospf-aggregate-states
clear-ddos-ospf-aggregate-statistics
clear-ddos-ospf-states
clear-ddos-ospf-statistics
clear-ddos-ospfv3v6-aggregate-states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear-ddos-ospfv3v6-aggregate-statistics
clear ddos-protection protocols ospfv3v6 states
clear-ddos-ospfv3v6-states
clear ddos-protection protocols pimv6
clear-ddos-pim-statistics
clear ddos-protection protocols pim-ctrl
clear ddos-protection protocols pim-ctrl aggregate
clear ddos-protection protocols pim-ctrl aggregate culprit-flows
<clear-ddos-pim-ctrl-aggregate-flows>
clear ddos-protection protocols pim-ctrl aggregate states
<clear-ddos-pim-ctrl-aggregate-states>
clear ddos-protection protocols pim-ctrl aggregate statistics
<clear-ddos-pim-ctrl-aggregate-statistics>
clear ddos-protection protocols pim-ctrl culprit-flows
<clear-ddos-pim-ctrl-flows>
clear ddos-protection protocols pim-ctrl states
<clear-ddos-pim-ctrl-states>
clear ddos-protection protocols pim-ctrl statistics
<clear-ddos-pim-ctrl-statistics>
clear ddos-protection protocols pim-data
clear ddos-protection protocols pim-data aggregate
clear ddos-protection protocols pim-data aggregate culprit-flows
<clear-ddos-pim-data-aggregate-flows>
clear ddos-protection protocols pim-data aggregate states
<clear-ddos-pim-data-aggregate-states>
clear ddos-protection protocols pim-data aggregate statistics
```

```

<clear-ddos-pim-data-aggregate-statistics>
clear ddos-protection protocols pim-data culprit-flows
<clear-ddos-pim-data-flows>
clear ddos-protection protocols pim-data states
<clear-ddos-pim-data-states>
clear ddos-protection protocols pim-data statistics
<clear-ddos-pim-data-statistics>
clear ddos-protection protocols pfe-alive
clear ddos-protection protocols pfe-alive aggregate
clear ddos-protection protocols pfe-alive aggregate states
clear-ddos-pfe-alive-aggregate-states
clear ddos-protection protocols pfe-alive aggregate statistics
clear ddos-protection protocols pfe-alive culprit-flows
clear ddos-protection protocols pfe-alive states
clear-ddos-pfe-alive-states
clear ddos-protection protocols pfe-alive statistics
clear-ddos-pfe-alive-statistics
clear ddos-protection protocols pim
clear ddos-protection protocols pim aggregate
clear ddos-protection protocols pim aggregate states
clear-ddos-pim-aggregate-states
clear ddos-protection protocols pim aggregate statistics
clear ddos-protection protocols pim culprit-flows
clear ddos-protection protocols pim states
clear-ddos-pim-states
clear ddos-protection protocols pim statistics
clear-ddos-pim-statistics
clear ddos-protection protocols pimv6
clear ddos-protection protocols pimv6 aggregate
clear ddos-protection protocols pimv6 aggregate culprit-flows
clear ddos-protection protocols pimv6 aggregate states
clear ddos-protection protocols pimv6 aggregate statistics
clear ddos-protection protocols pimv6 states
clear ddos-protection protocols pimv6 statistics
clear ddos-protection protocols pmvrp
clear ddos-protection protocols pmvrp aggregate
clear ddos-protection protocols pmvrp aggregate states
clear-ddos-pmvrp-aggregate-states
clear ddos-protection protocols pmvrp aggregate statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp states
clear-ddos-pmvrp-states
clear ddos-protection protocols pmvrp statistics
clear-ddos-pmvrp-statistics
clear ddos-protection protocols pos
clear ddos-protection protocols pos aggregate
clear ddos-protection protocols pos aggregate states
clear-ddos-pos-aggregate-states
clear ddos-protection protocols pos aggregate statistics
clear-ddos-pos-aggregate-statistics
clear ddos-protection protocols pos states
clear-ddos-pos-states
clear ddos-protection protocols pos statistics
clear-ddos-pos-statistics
clear ddos-protection protocols ppp

```

```
clear ddos-protection protocols ppp aggregate
clear ddos-protection protocols ppp aggregate states
clear-ddos-ppp-aggregate-states
clear ddos-protection protocols ppp aggregate statistics
clear-ddos-ppp-aggregate-statistics
clear ddos-protection protocols ppp authentication
clear ddos-protection protocols ppp authentication states
clear-ddos-ppp-auth-states
clear ddos-protection protocols ppp authentication statistics
clear-ddos-ppp-auth-statistics
clear ddos-protection protocols ppp ipcp
clear ddos-protection protocols ppp ipcp states
clear-ddos-ppp-ipcp-states
clear ddos-protection protocols ppp ipcp statistics
clear-ddos-ppp-ipcp-statistics
clear ddos-protection protocols ppp ipv6cp
clear ddos-protection protocols ppp ipv6cp states
clear-ddos-ppp-ipv6cp-states
clear ddos-protection protocols ppp ipv6cp statistics
clear-ddos-ppp-ipv6cp-statistics
clear ddos-protection protocols ppp isis
clear ddos-protection protocols ppp isis states
clear-ddos-ppp-isis-states
clear ddos-protection protocols ppp isis statistics
clear-ddos-ppp-isis-statistics
clear ddos-protection protocols ppp lcp
clear ddos-protection protocols ppp lcp states
clear-ddos-ppp-lcp-states
clear ddos-protection protocols ppp lcp statistics
clear-ddos-ppp-lcp-statistics
clear ddos-protection protocols ppp mplsdp
clear ddos-protection protocols ppp mplsdp states
clear-ddos-ppp-mplsdp-states
clear ddos-protection protocols ppp mplsdp statistics
clear-ddos-ppp-mplsdp-statistics
clear ddos-protection protocols ppp states
clear-ddos-ppp-states
clear ddos-protection protocols ppp statistics
clear-ddos-ppp-statistics
clear ddos-protection protocols ppp unclassified
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
<clear-ddos-ppp-unclass-statistics>
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
clear ddos-protection protocols pppoe aggregate states
clear-ddos-pppoe-aggregate-states
clear ddos-protection protocols pppoe aggregate statistics
clear-ddos-pppoe-aggregate-statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear-ddos-pppoe-padi-states
clear ddos-protection protocols pppoe padi statistics
clear-ddos-pppoe-padi-statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear-ddos-pppoe-padm-states
clear ddos-protection protocols pppoe padm statistics
clear-ddos-pppoe-padm-statistics
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
```

```
clear-ddos-pppoe-padn-states
clear ddos-protection protocols pppoe padn statistics
clear-ddos-pppoe-padn-statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear-ddos-pppoe-pado-states
clear ddos-protection protocols pppoe pado statistics
clear-ddos-pppoe-pado-statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear-ddos-pppoe-padr-states
clear ddos-protection protocols pppoe padr statistics
clear-ddos-pppoe-padr-statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear-ddos-pppoe-pads-states
clear ddos-protection protocols pppoe pads statistics
clear-ddos-pppoe-pads-statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear-ddos-pppoe-padt-states
clear ddos-protection protocols pppoe padt statistics
clear-ddos-pppoe-padt-statistics
clear ddos-protection protocols pppoe states
clear-ddos-pppoe-states
clear ddos-protection protocols pppoe statistics
clear-ddos-pppoe-statistics
clear ddos-protection protocols ptp
clear ddos-protection protocols ptp aggregate
clear ddos-protection protocols ptp aggregate states
clear-ddos-ptp-aggregate-states
clear ddos-protection protocols ptp aggregate statistics
clear-ddos-ptp-aggregate-statistics
clear ddos-protection protocols ptp states
clear-ddos-ptp-states
clear ddos-protection protocols ptp statistics
clear-ddos-ptp-statistics
clear ddos-protection protocols pvstp
clear ddos-protection protocols pvstp aggregate
clear ddos-protection protocols pvstp aggregate states
clear-ddos-pvstp-aggregate-states
clear ddos-protection protocols pvstp aggregate statistics
clear-ddos-pvstp-aggregate-statistics
clear ddos-protection protocols pvstp states
clear-ddos-pvstp-states
clear ddos-protection protocols pvstp statistics
clear-ddos-pvstp-statistics
clear ddos-protection protocols radius
clear ddos-protection protocols radius accounting
clear ddos-protection protocols radius accounting states
clear-ddos-radius-account-states
clear ddos-protection protocols radius accounting statistics
clear-ddos-radius-account-statistics
clear ddos-protection protocols radius aggregate
clear ddos-protection protocols radius aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius aggregate statistics
clear-ddos-radius-aggregate-statistics
clear ddos-protection protocols radius authorization
clear ddos-protection protocols radius authorization states
clear ddos-protection protocols radius authorization statistics
```

```
clear-ddos-ospfv3v6-statistics
clear-ddos-pfe-alive-aggregate-states
clear-ddos-pfe-alive-aggregate-statistics
clear-ddos-pfe-alive-states
clear-ddos-pfe-alive-statistics
clear-ddos-pim-aggregate-states
clear-ddos-pim-aggregate-statistics
clear-ddos-pim-states
clear-ddos-pmvrp-aggregate-states
clear-ddos-pmvrp-aggregate-statistics
clear-ddos-pmvrp-states
clear-ddos-pmvrp-statistics
clear-ddos-pos-aggregate-states
clear-ddos-pos-aggregate-statistics
clear-ddos-pos-states
clear-ddos-pos-statistics
clear-ddos-ppp-aggregate-states
clear-ddos-ppp-aggregate-statistics
clear-ddos-ppp-auth-states
clear-ddos-ppp-ipcp-states
clear-ddos-ppp-ipcp-statistics
clear-ddos-ppp-ipv6cp-states
clear-ddos-ppp-ipv6cp-statistics
clear-ddos-ppp-isis-states
clear-ddos-ppp-isis-statistics
clear-ddos-ppp-lcp-states
clear-ddos-ppp-lcp-statistics
clear-ddos-ppp-mplscp-states
clear-ddos-ppp-mplscp-statistics
clear-ddos-pppoe-aggregate-states
clear-ddos-pppoe-aggregate-statistics
clear-ddos-pppoe-padi-states
clear-ddos-pppoe-padi-statistics
clear-ddos-pppoe-padm-states
clear-ddos-pppoe-padm-statistics
clear-ddos-pppoe-padn-states
clear-ddos-pppoe-padn-statistics
clear-ddos-pppoe-pado-states
clear-ddos-pppoe-pado-statistics
clear-ddos-pppoe-padr-states
clear-ddos-pppoe-padr-statistics
clear-ddos-pppoe-pads-states
clear-ddos-pppoe-pads-statistics
clear-ddos-pppoe-padt-states
clear-ddos-pppoe-padt-statistics
clear-ddos-pppoe-states
clear-ddos-pppoe-statistics
clear-ddos-ppp-states
clear-ddos-ppp-statistics
clear-ddos-ptp-aggregate-states
clear-ddos-ptp-aggregate-statistics
clear-ddos-ptp-states
clear-ddos-ptp-statistics
clear-ddos-pvstp-aggregate-states
clear-ddos-pvstp-aggregate-statistics
clear-ddos-pvstp-states
clear-ddos-pvstp-statistics
clear-ddos-radius-account-states
clear-ddos-radius-account-statistics
clear-ddos-radius-aggregate-states
clear-ddos-radius-aggregate-statistics
```

```
clear-ddos-radius-auth-states
clear ddos-protection protocols radius authorization statistics
clear-ddos-radius-auth-statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols radius server
clear ddos-protection protocols radius server states
clear-ddos-radius-server-states
clear ddos-protection protocols radius server statistics
clear-ddos-radius-server-statistics
clear ddos-protection protocols radius states
clear-ddos-radius-states
clear ddos-protection protocols radius statistics
clear-ddos-radius-statistics
clear ddos-protection protocols redirect
clear ddos-protection protocols redirect aggregate
clear ddos-protection protocols redirect aggregate states
clear-ddos-redirect-aggregate-states
clear ddos-protection protocols redirect aggregate statistics
clear-ddos-redirect-aggregate-statistics
clear ddos-protection protocols redirect states
clear-ddos-redirect-states
clear ddos-protection protocols redirect statistics
clear-ddos-redirect-statistics
clear ddos-protection protocols reject
clear ddos-protection protocols reject aggregate
clear ddos-protection protocols reject aggregate states
clear ddos-protection protocols reject aggregate statistics
clear ddos-protection protocols reject states
clear ddos-protection protocols reject statistics
clear ddos-protection protocols rip
clear ddos-protection protocols rip aggregate
clear ddos-protection protocols rip aggregate states
clear-ddos-rip-aggregate-states
clear ddos-protection protocols rip aggregate statistics
clear-ddos-rip-aggregate-statistics
clear ddos-protection protocols rip states
clear-ddos-rip-states
clear ddos-protection protocols rip statistics
clear-ddos-rip-statistics
clear ddos-protection protocols ripv6
clear ddos-protection protocols ripv6 aggregate
clear ddos-protection protocols ripv6 aggregate states
clear-ddos-ripv6-aggregate-states
clear ddos-protection protocols ripv6 aggregate statistics
clear-ddos-ripv6-aggregate-statistics
clear ddos-protection protocols ripv6 states
clear-ddos-ripv6-states
clear ddos-protection protocols ripv6 statistics
clear-ddos-ripv6-statistics
clear ddos-protection protocols rsvp
clear ddos-protection protocols rsvp aggregate
clear ddos-protection protocols rsvp aggregate states
clear-ddos-rsvp-aggregate-states
clear ddos-protection protocols rsvp aggregate statistics
clear-ddos-rsvp-aggregate-statistics
clear ddos-protection protocols rsvp states
clear-ddos-rsvp-states
clear ddos-protection protocols rsvp statistics
clear-ddos-rsvp-statistics
clear ddos-protection protocols rsvpv6
clear ddos-protection protocols rsvpv6 aggregate
```

```
clear ddos-protection protocols rsvpv6 aggregate states
clear-ddos-rsvpv6-aggregate-states
clear ddos-protection protocols rsvpv6 aggregate statistics
clear-ddos-rsvpv6-aggregate-statistics
clear ddos-protection protocols rsvpv6 states
clear-ddos-rsvpv6-states
clear ddos-protection protocols rsvpv6 statistics
clear-ddos-rsvpv6-statistics
clear ddos-protection protocols sample
clear ddos-protection protocols sample aggregate
clear ddos-protection protocols sample aggregate states
<clear-ddos-sample-aggregate-states>
clear ddos-protection protocols sample aggregate statistics
<clear-ddos-sample-aggregate-statistics>
clear ddos-protection protocols sample host
clear ddos-protection protocols sample host states
<clear-ddos-sample-host-states>
clear ddos-protection protocols sample host statistics
<clear-ddos-sample-host-statistics>
clear ddos-protection protocols sample pfe
clear ddos-protection protocols sample pfe culprit-flows
clear ddos-protection protocols sample pfe states
<clear-ddos-sample-pfe-states>
clear ddos-protection protocols sample pfe statistics
clear ddos-protection protocols sample sflow
clear ddos-protection protocols sample sflow culprit-flows
<clear-ddos-sample-sflow-flows>
clear ddos-protection protocols sample sflow states
<clear-ddos-sample-sflow-states>
clear ddos-protection protocols sample sflow statistics
<clear-ddos-sample-sflow-statistics>
clear ddos-protection protocols sample states
<clear-ddos-sample-states>
clear ddos-protection protocols sample statistics
<clear-ddos-sample-statistics>
clear ddos-protection protocols sample syslog
clear ddos-protection protocols sample syslog culprit-flows
clear ddos-protection protocols sample syslog states
<clear-ddos-sample-syslog-states>
clear ddos-protection protocols sample syslog statistics
<clear-ddos-sample-syslog-statistics>
clear ddos-protection protocols sample tap
clear ddos-protection protocols sample tap states
clear ddos-protection protocols sample-dest
clear ddos-protection protocols sample-dest aggregate
clear ddos-protection protocols sample-dest aggregate culprit-flows
<clear-ddos-sample-dest-aggregate-flows>
clear ddos-protection protocols sample-dest aggregate states
<clear-ddos-sample-dest-aggregate-states>
clear ddos-protection protocols sample-dest aggregate statistics
<clear-ddos-sample-dest-aggregate-statistics>
clear ddos-protection protocols sample-dest culprit-flows
<clear-ddos-sample-dest-flows>
clear ddos-protection protocols sample-dest states
<clear-ddos-sample-dest-states>
clear ddos-protection protocols sample-dest statistics
<clear-ddos-sample-dest-statistics>
clear ddos-protection protocols sample-source
clear ddos-protection protocols sample-source aggregate
clear ddos-protection protocols sample-source aggregate culprit-flows
<clear-ddos-sample-source-aggregate-flows>
```



```

clear ddos-protection protocols sample-source aggregate states
<clear-ddos-sample-source-aggregate-states>
clear ddos-protection protocols sample-source aggregate statistics
<clear-ddos-sample-source-aggregate-statistics>
clear ddos-protection protocols sample-source culprit-flows
<clear-ddos-sample-source-flows>
clear ddos-protection protocols sample-source states
<clear-ddos-sample-source-states>
clear ddos-protection protocols sample-source statistics
<clear-ddos-sample-source-statistics>
clear ddos-protection protocols sample tap statistics
<clear-ddos-sample-tap-statistics>
clear ddos-protection protocols services
clear ddos-protection protocols services aggregate
clear ddos-protection protocols services aggregate states
clear-ddos-services-aggregate-states
clear ddos-protection protocols services aggregate statistics
clear ddos-protection protocols services bsdt
clear ddos-protection protocols services bsdt culprit-flows
<clear-ddos-services-BSDT-flows>
clear ddos-protection protocols services bsdt states
<clear-ddos-services-BSDT-states>
clear ddos-protection protocols services bsdt statistics
<clear-ddos-services-BSDT-statistics>
clear ddos-protection protocols services culprit-flows
<clear-ddos-services-flows>
clear ddos-protection protocols services packet
clear ddos-protection protocols services packet culprit-flows
<clear-ddos-services-packet-flows>
clear ddos-protection protocols services packet states
<clear-ddos-services-packet-states>
clear ddos-protection protocols services packet statistics
<clear-ddos-services-packet-statistics>
clear ddos-protection protocols services states
clear-ddos-services-states
clear ddos-protection protocols services statistics
clear-ddos-services-statistics
clear ddos-protection protocols snmp
clear ddos-protection protocols snmp aggregate
clear ddos-protection protocols snmp aggregate states
clear-ddos-snmp-aggregate-states
clear ddos-protection protocols snmp aggregate statistics
clear ddos-protection protocols snmp culprit-flows
clear ddos-protection protocols snmp states
clear-ddos-snmp-states
clear ddos-protection protocols snmp statistics
clear-ddos-snmp-statistics
clear ddos-protection protocols snmpv6
clear ddos-protection protocols snmpv6 aggregate
clear ddos-protection protocols snmpv6 aggregate states
clear-ddos-snmpv6-aggregate-states
clear ddos-protection protocols snmpv6 aggregate statistics
clear-ddos-snmpv6-aggregate-statistics
clear ddos-protection protocols snmpv6 states
clear-ddos-snmpv6-states
clear ddos-protection protocols snmpv6 statistics
clear-ddos-snmpv6-statistics
clear ddos-protection protocols ssh
clear ddos-protection protocols ssh aggregate
clear ddos-protection protocols ssh aggregate states
clear-ddos-ssh-aggregate-states

```

```
clear ddos-protection protocols ssh aggregate statistics
clear-ddos-ssh-aggregate-statistics
clear ddos-protection protocols ssh states
clear-ddos-ssh-states
clear ddos-protection protocols ssh statistics
clear-ddos-ssh-statistics
clear ddos-protection protocols sshv6
clear ddos-protection protocols sshv6 aggregate
clear ddos-protection protocols sshv6 aggregate states
clear-ddos-sshv6-aggregate-states
clear ddos-protection protocols sshv6 aggregate statistics
clear ddos-protection protocols sshv6 culprit-flows
clear ddos-protection protocols sshv6 states
clear-ddos-sshv6-states
clear ddos-protection protocols sshv6 statistics
clear-ddos-sshv6-statistics
clear ddos-protection protocols states
clear-ddos-protocols-states
clear ddos-protection protocols statistics
clear-ddos-protocols-statistics
clear ddos-protection protocols stp
clear ddos-protection protocols stp aggregate
clear ddos-protection protocols stp aggregate states
clear-ddos-stp-aggregate-states
clear ddos-protection protocols stp aggregate statistics
clear-ddos-stp-aggregate-statistics
clear ddos-protection protocols stp states
clear-ddos-stp-states
clear ddos-protection protocols stp statistics
clear-ddos-stp-statistics
clear ddos-protection protocols tacacs
clear ddos-protection protocols tacacs aggregate
clear ddos-protection protocols tacacs aggregate states
clear-ddos-tacacs-aggregate-states
clear ddos-protection protocols tacacs aggregate statistics
clear-ddos-tacacs-aggregate-statistics
clear ddos-protection protocols tacacs states
clear-ddos-tacacs-states
clear ddos-protection protocols tacacs statistics
clear-ddos-tacacs-statistics
clear ddos-protection protocols tcp-flags
clear ddos-protection protocols tcp-flags aggregate
clear ddos-protection protocols tcp-flags aggregate states
clear-ddos-tcp-flags-aggregate-states
clear ddos-protection protocols tcp-flags aggregate statistics
clear-ddos-tcp-flags-aggregate-statistics
clear ddos-protection protocols tcp-flags established
clear ddos-protection protocols tcp-flags established states
clear-ddos-tcp-flags-establish-states
clear ddos-protection protocols tcp-flags established statistics
clear-ddos-tcp-flags-establish-statistics
clear ddos-protection protocols tcp-flags initial
clear ddos-protection protocols tcp-flags initial culprit-flows
clear ddos-protection protocols tcp-flags initial states
clear-ddos-tcp-flags-initial-states
clear ddos-protection protocols tcp-flags initial statistics
clear-ddos-tcp-flags-initial-statistics
clear ddos-protection protocols tcp-flags states
clear-ddos-tcp-flags-states
clear ddos-protection protocols tcp-flags statistics
clear-ddos-tcp-flags-statistics
```

```
clear ddos-protection protocols tcp-flags unclassified
clear ddos-protection protocols tcp-flags unclassified states
clear-ddos-tcp-flags-unclass-states
clear ddos-protection protocols tcp-flags unclassified statistics
clear-ddos-tcp-flags-unclass-statistics
clear ddos-protection protocols telnet
clear ddos-protection protocols telnet aggregate
clear ddos-protection protocols telnet aggregate culprit-flows
clear ddos-protection protocols telnet aggregate states
clear-ddos-telnet-aggregate-states
clear ddos-protection protocols telnet aggregate statistics
clear-ddos-telnet-aggregate-statistics
clear ddos-protection protocols telnet states
clear-ddos-telnet-states
clear ddos-protection protocols telnet statistics
clear-ddos-telnet-statistics
clear ddos-protection protocols telnetv6
clear ddos-protection protocols telnetv6 aggregate
clear ddos-protection protocols telnetv6 aggregate states
clear-ddos-telnetv6-aggregate-states
clear ddos-protection protocols telnetv6 aggregate statistics
clear-ddos-telnetv6-aggregate-statistics
clear ddos-protection protocols telnetv6 states
clear-ddos-telnetv6-states
clear ddos-protection protocols telnetv6 statistics
clear-ddos-telnetv6-statistics
clear ddos-protection protocols ttl
clear ddos-protection protocols ttl aggregate
clear ddos-protection protocols ttl aggregate culprit-flows
clear ddos-protection protocols ttl aggregate states
clear-ddos-ttl-aggregate-states
clear ddos-protection protocols ttl aggregate statistics
clear-ddos-ttl-aggregate-statistics
clear ddos-protection protocols ttl states
clear-ddos-ttl-states
clear ddos-protection protocols ttl statistics
clear-ddos-ttl-statistics
clear ddos-protection protocols tunnel-fragment
clear ddos-protection protocols tunnel-fragment aggregate
clear ddos-protection protocols tunnel-fragment aggregate states
clear-ddos-tun-frag-aggregate-states
clear ddos-protection protocols tunnel-fragment aggregate statistics
clear-ddos-tun-frag-aggregate-statistics
clear ddos-protection protocols tunnel-fragment states
clear-ddos-tun-frag-states
clear ddos-protection protocols tunnel-fragment statistics
clear-ddos-tun-frag-statistics
clear ddos-protection protocols unclassified
clear ddos-protection protocols unclassified aggregate
clear ddos-protection protocols unclassified aggregate states
clear ddos-protection protocols unclassified aggregate statistics
clear ddos-protection protocols unclassified control-layer2
clear ddos-protection protocols unclassified control-layer2 culprit-flows
clear ddos-protection protocols unclassified control-layer2 states
clear ddos-protection protocols unclassified control-layer2 statistics
clear ddos-protection protocols unclassified control-v4
clear ddos-protection protocols unclassified control-v4 culprit-flows
clear ddos-protection protocols unclassified control-v4 states
clear ddos-protection protocols unclassified control-v4 statistics
clear ddos-protection protocols unclassified control-v6
clear ddos-protection protocols unclassified control-v6 culprit-flows
```

```
clear ddos-protection protocols unclassified control-v6 states
clear ddos-protection protocols unclassified control-v6 statistics
clear ddos-protection protocols unclassified filter-v4 culprit-flows
clear ddos-protection protocols unclassified filter-v4 states
clear ddos-protection protocols unclassified filter-v4 statistics
clear ddos-protection protocols unclassified filter-v6
clear ddos-protection protocols unclassified filter-v6 culprit-flows
clear ddos-protection protocols unclassified filter-v6 states
clear ddos-protection protocols unclassified filter-v6 statistics
clear ddos-protection protocols unclassified fw-host
clear ddos-protection protocols unclassified fw-host culprit-flows
<clear-ddos-uncls-fw-host-flows>
clear ddos-protection protocols unclassified fw-host states
<clear-ddos-uncls-fw-host-states>
clear ddos-protection protocols unclassified fw-host statistics
<clear-ddos-uncls-fw-host-statistics>
clear ddos-protection protocols unclassified host-route-v4
clear ddos-protection protocols unclassified host-route-v4 culprit-flows
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 statistics
clear ddos-protection protocols unclassified host-route-v6
clear ddos-protection protocols unclassified host-route-v6 culprit-flows
clear ddos-protection protocols unclassified host-route-v6 states
clear ddos-protection protocols unclassified host-route-v6 statistics
clear ddos-protection protocols unclassified mcast-copy
clear ddos-protection protocols unclassified mcast-copy culprit-flows
<clear-ddos-uncls-mcast-copy-flows>
clear ddos-protection protocols unclassified mcast-copy states
<clear-ddos-uncls-mcast-copy-states>
clear ddos-protection protocols unclassified mcast-copy statistics
<clear-ddos-uncls-mcast-copy-statistics>
clear ddos-protection protocols unknown-l2mc
clear ddos-protection protocols unknown-l2mc aggregate
clear ddos-protection protocols unknown-l2mc aggregate culprit-flows
<clear-ddos-unknown-l2mc-aggregate-flows>
clear ddos-protection protocols unknown-l2mc aggregate states
<clear-ddos-unknown-l2mc-aggregate-states>
clear ddos-protection protocols unknown-l2mc aggregate statistics
<clear-ddos-unknown-l2mc-aggregate-statistics>
clear ddos-protection protocols unknown-l2mc culprit-flows
<clear-ddos-unknown-l2mc-flows>
clear ddos-protection protocols unknown-l2mc states
<clear-ddos-unknown-l2mc-states>
clear ddos-protection protocols unknown-l2mc statistics
<clear-ddos-unknown-l2mc-statistics>
clear ddos-protection protocols urpf-fail
clear ddos-protection protocols urpf-fail aggregate
clear ddos-protection protocols urpf-fail aggregate culprit-flows
<clear-ddos-urpf-fail-aggregate-flows>
clear ddos-protection protocols urpf-fail aggregate states
<clear-ddos-urpf-fail-aggregate-states>
clear ddos-protection protocols urpf-fail aggregate statistics
<clear-ddos-urpf-fail-aggregate-statistics>
clear ddos-protection protocols urpf-fail culprit-flows
<clear-ddos-urpf-fail-flows>
clear ddos-protection protocols urpf-fail states
<clear-ddos-urpf-fail-states>
clear ddos-protection protocols urpf-fail statistics
<clear-ddos-urpf-fail-statistics>
clear ddos-protection protocols vcipc-udp
```

```

clear ddos-protection protocols vcipc-udp aggregate
clear ddos-protection protocols vcipc-udp aggregate culprit-flows
<clear-ddos-vcipc-udp-aggregate-flows>
clear ddos-protection protocols vcipc-udp aggregate states
<clear-ddos-vcipc-udp-aggregate-states>
clear ddos-protection protocols vcipc-udp aggregate statistics
<clear-ddos-vcipc-udp-aggregate-statistics>
clear ddos-protection protocols vcipc-udp culprit-flows
<clear-ddos-vcipc-udp-flows>
clear ddos-protection protocols vcipc-udp states
<clear-ddos-vcipc-udp-states>
<clear-ddos-vcipc-udp-statistics>
clear ddos-protection protocols unclassified other
clear ddos-protection protocols unclassified other culprit-flows
clear ddos-protection protocols unclassified other states
clear ddos-protection protocols unclassified other statistics
clear ddos-protection protocols unclassified resolve-v4
clear ddos-protection protocols unclassified resolve-v4 culprit-flows
clear ddos-protection protocols unclassified resolve-v4 states
clear ddos-protection protocols unclassified resolve-v4 statistics
clear ddos-protection protocols unclassified resolve-v6
clear ddos-protection protocols unclassified resolve-v6 culprit-flows
clear ddos-protection protocols unclassified resolve-v6 states
clear ddos-protection protocols unclassified resolve-v6 statistics
clear ddos-protection protocols unclassified states
clear ddos-protection protocols unclassified statistics
<clear-ddos-uncls-statistics>
clear ddos-protection protocols virtual-chassis
clear ddos-protection protocols virtual-chassis aggregate
clear ddos-protection protocols virtual-chassis aggregate culprit-flows
clear ddos-protection protocols virtual-chassis aggregate states
clear-ddos-protocols-states
clear-ddos-protocols-statistics
clear-ddos-radius-server-states
clear-ddos-radius-server-statistics
clear-ddos-radius-states
clear-ddos-radius-statistics
clear ddos-protection protocols re-services
clear ddos-protection protocols re-services aggregate
clear ddos-protection protocols re-services aggregate culprit-flows
<clear-ddos-re-services-aggregate-flows>
clear ddos-protection protocols re-services aggregate states
<clear-ddos-re-services-aggregate-states>
clear ddos-protection protocols re-services aggregate statistics
<clear-ddos-re-services-aggregate-statistics>
clear ddos-protection protocols re-services captive-portal
clear ddos-protection protocols re-services captive-portal culprit-flows
<clear-ddos-re-services-captive-portal-flows>
clear ddos-protection protocols re-services captive-portal states
<clear-ddos-re-services-captive-portal-states>
clear ddos-protection protocols re-services captive-portal statistics
<clear-ddos-re-services-captive-portal-statistics>
clear ddos-protection protocols re-services culprit-flows
<clear-ddos-re-services-flows>
clear ddos-protection protocols re-services states
<clear-ddos-re-services-states>
clear ddos-protection protocols re-services statistics
<clear-ddos-re-services-statistics>
clear ddos-protection protocols re-services-v6
clear ddos-protection protocols re-services-v6 aggregate
clear ddos-protection protocols re-services-v6 aggregate culprit-flows

```

```
<clear-ddos-re-services-v6-aggregate-flows>
clear ddos-protection protocols re-services-v6 aggregate states
<clear-ddos-re-services-v6-aggregate-states>
clear ddos-protection protocols re-services-v6 aggregate statistics
<clear-ddos-re-services-v6-aggregate-statistics>
clear ddos-protection protocols re-services-v6 captive-portal
clear ddos-protection protocols re-services-v6 captive-portal culprit-flows
<clear-ddos-re-services-v6-captive-portal-v6-flows>
clear ddos-protection protocols re-services-v6 captive-portal states
<clear-ddos-re-services-v6-captive-portal-v6-states>
clear ddos-protection protocols re-services-v6 captive-portal statistics
<clear-ddos-re-services-v6-captive-portal-v6-statistics>
clear ddos-protection protocols re-services-v6 culprit-flows
<clear-ddos-re-services-v6-flows>
clear ddos-protection protocols re-services-v6 states
<clear-ddos-re-services-v6-states>
clear ddos-protection protocols re-services-v6 statistics
<clear-ddos-re-services-v6-statistics>
clear-ddos-redirect-aggregate-states
clear-ddos-redirect-states
clear-ddos-redirect-statistics
clear-ddos-rip-aggregate-states
clear-ddos-rip-aggregate-statistics
clear-ddos-rip-states
clear-ddos-rip-statistics
clear-ddos-ripv6-aggregate-states
clear-ddos-ripv6-aggregate-statistics
clear-ddos-ripv6-states
clear-ddos-ripv6-statistics
clear-ddos-rsvp-aggregate-states
clear-ddos-rsvp-aggregate-statistics
clear-ddos-rsvp-states
clear-ddos-rsvp-statistics
clear-ddos-rsvpv6-aggregate-states
clear-ddos-rsvpv6-aggregate-statistics
clear-ddos-rsvpv6-states
clear-ddos-rsvpv6-statistics
clear-ddos-services-aggregate-states
clear-ddos-services-aggregate-statistics
clear-ddos-services-states
clear-ddos-services-statistics
clear-ddos-snmp-aggregate-states
clear-ddos-snmp-aggregate-statistics
clear-ddos-snmp-states
clear-ddos-snmp-statistics
clear-ddos-snmppv6-aggregate-states
clear-ddos-snmppv6-aggregate-statistics
clear-ddos-snmppv6-states
clear-ddos-snmppv6-statistics
clear-ddos-ssh-aggregate-states
clear-ddos-ssh-aggregate-statistics
clear-ddos-ssh-states
clear-ddos-ssh-statistics
clear-ddos-sshv6-aggregate-states
clear-ddos-sshv6-aggregate-statistics
clear-ddos-sshv6-states
clear-ddos-sshv6-statistics
clear-ddos-stp-aggregate-states
clear-ddos-stp-aggregate-statistics
clear-ddos-stp-states
clear-ddos-stp-statistics
```

```
clear ddos-protection protocols syslog
clear ddos-protection protocols syslog aggregate
clear ddos-protection protocols syslog aggregate culprit-flows
<clear-ddos-syslog-aggregate-flows>
clear ddos-protection protocols syslog aggregate states
<clear-ddos-syslog-aggregate-states>
clear ddos-protection protocols syslog aggregate statistics
<clear-ddos-syslog-aggregate-statistics>
clear ddos-protection protocols syslog culprit-flows
<clear-ddos-syslog-flows>
clear ddos-protection protocols syslog states
<clear-ddos-syslog-states>
clear ddos-protection protocols syslog statistics
<clear-ddos-syslog-statistics>
clear-ddos-tacacs-aggregate-states
clear-ddos-tacacs-aggregate-statistics
clear-ddos-tacacs-states
clear-ddos-tacacs-statistics
clear-ddos-tcp-flags-aggregate-states
clear-ddos-tcp-flags-aggregate-statistics
clear-ddos-tcp-flags-establish-states
clear-ddos-tcp-flags-establish-statistics
clear-ddos-tcp-flags-initial-states
clear-ddos-tcp-flags-initial-statistics
clear-ddos-tcp-flags-states
clear-ddos-tcp-flags-statistics
clear-ddos-tcp-flags-unclass-states
clear-ddos-tcp-flags-unclass-statistics
clear-ddos-telnet-aggregate-states
clear-ddos-telnet-aggregate-statistics
clear-ddos-telnet-states
clear-ddos-telnet-statistics
clear-ddos-telnetv6-aggregate-states
clear-ddos-telnetv6-aggregate-statistics
clear-ddos-telnetv6-states
clear-ddos-telnetv6-statistics
clear-ddos-ttl-aggregate-states
clear-ddos-ttl-aggregate-statistics
clear-ddos-ttl-states
clear-ddos-ttl-statistics
clear-ddos-tun-frag-aggregate-states
clear-ddos-tun-frag-aggregate-statistics
clear-ddos-tun-frag-states
clear-ddos-tun-frag-statistics
clear ddos-protection protocols tunnel-ka
clear ddos-protection protocols tunnel-ka aggregate
clear ddos-protection protocols tunnel-ka aggregate culprit-flows
<clear-ddos-tunnel-ka-aggregate-flows>
clear ddos-protection protocols tunnel-ka aggregate states
<clear-ddos-tunnel-ka-aggregate-states>
clear ddos-protection protocols tunnel-ka aggregate statistics
<clear-ddos-tunnel-ka-aggregate-statistics>
clear ddos-protection protocols tunnel-ka culprit-flows
<clear-ddos-tunnel-ka-flows>
clear ddos-protection protocols tunnel-ka states
<clear-ddos-tunnel-ka-states>
clear ddos-protection protocols tunnel-ka statistics
<clear-ddos-tunnel-ka-statistics>
clear-ddos-vchassis-aggregate-states
clear ddos-protection protocols virtual-chassis aggregate statistics
clear-ddos-vchassis-aggregate-statistics
```

```
clear ddos-protection protocols virtual-chassis control-high
clear ddos-protection protocols virtual-chassis control-high states
clear-ddos-vchassis-control-hi-states
clear ddos-protection protocols virtual-chassis control-high statistics
clear-ddos-vchassis-control-hi-statistics
clear ddos-protection protocols virtual-chassis control-low
clear ddos-protection protocols virtual-chassis control-low states
clear-ddos-vchassis-control-lo-states
clear ddos-protection protocols virtual-chassis control-low statistics
clear-ddos-vchassis-control-lo-statistics
clear ddos-protection protocols virtual-chassis states
clear-ddos-vchassis-states
clear ddos-protection protocols virtual-chassis statistics
clear-ddos-vchassis-statistics
clear ddos-protection protocols virtual-chassis unclassified
clear ddos-protection protocols virtual-chassis unclassified culprit-flows
clear ddos-protection protocols virtual-chassis unclassified states
clear-ddos-vchassis-unclass-states
clear ddos-protection protocols virtual-chassis unclassified statistics
clear-ddos-vchassis-unclass-statistics
clear ddos-protection protocols virtual-chassis vc-packets
clear ddos-protection protocols virtual-chassis vc-packets states
clear-ddos-vchassis-vc-packets-states
clear ddos-protection protocols virtual-chassis vc-packets statistics
clear-ddos-vchassis-vc-packets-statistics
clear ddos-protection protocols virtual-chassis vc-ttl-errors
clear ddos-protection protocols virtual-chassis vc-ttl-errors states
clear-ddos-vchassis-vc-ttl-err-states
clear ddos-protection protocols virtual-chassis vc-ttl-errors statistics
clear-ddos-vchassis-vc-ttl-err-statistics
clear ddos-protection protocols vrrp
clear ddos-protection protocols vrrp aggregate
clear ddos-protection protocols vrrp aggregate states
clear-ddos-vrrp-aggregate-states
clear ddos-protection protocols vrrp aggregate statistics
clear ddos-protection protocols vrrp culprit-flows
clear ddos-protection protocols vrrp statistics
clear-ddos-vrrp-statistics
clear ddos-protection protocols vrrpv6
clear ddos-protection protocols vrrpv6 aggregate
clear ddos-protection protocols vrrpv6 aggregate states
clear-ddos-vrrpv6-aggregate-states
clear ddos-protection protocols vrrpv6 aggregate statistics
clear-ddos-vrrpv6-aggregate-statistics
clear ddos-protection protocols vrrpv6 states
clear-ddos-vrrpv6-states
clear ddos-protection protocols vrrpv6 statistics
clear-ddos-uncls-host-rt-v4-flows
clear-ddos-vchassis-aggregate-statistics
clear-ddos-vchassis-control-hi-states
clear-ddos-vchassis-control-hi-statistics
clear-ddos-vchassis-control-lo-states
clear-ddos-vchassis-control-lo-statistics
clear-ddos-vchassis-states
clear-ddos-vchassis-statistics
clear-ddos-vchassis-unclass-states
clear-ddos-vchassis-unclass-statistics
clear-ddos-vchassis-vc-packets-states
clear-ddos-vchassis-vc-packets-statistics
clear-ddos-vchassis-vc-ttl-err-states
clear-ddos-vchassis-vc-ttl-err-statistics
```



```

clear-ddos-vrrp-aggregate-states
clear-ddos-vrrp-aggregate-statistics
clear-ddos-vrrp-states
clear-ddos-vrrp-statistics
clear-ddos-vrrpv6-aggregate-states
clear-ddos-vrrpv6-aggregate-statistics
clear-ddos-vrrpv6-states
clear-ddos-vrrpv6-statistics
clear ddos-protection protocols vxlan
clear ddos-protection protocols vxlan aggregate
clear ddos-protection protocols vxlan aggregate culprit-flows
clear-ddos-vxlan-aggregate-flows
clear ddos-protection protocols vxlan aggregate states
<clear-ddos-vxlan-aggregate-states>
clear ddos-protection protocols vxlan aggregate statistics
<clear-ddos-vxlan-aggregate-statistics>
clear ddos-protection protocols vxlan culprit-flows
<clear-ddos-vxlan-flows>
clear ddos-protection protocols vxlan states
<clear-ddos-vxlan-states>
clear ddos-protection protocols vxlan statistics
<clear-ddos-vxlan-statistics>
clear dhcp
clear dhcp client
clear dhcp client binding
<clear-dhcp-client-binding-information>
clear dhcp client statistics
<clear-client-statistics-information>
clear dhcp proxy-client
clear dhcp proxy-client statistics
clear dhcp relay
clear dhcp relay binding
<clear-dhcp-relay-binding-information>
clear dhcp relay binding interface
<clear-dhcp-interface-bindings>
clear dhcp relay statistics
<clear-dhcp-relay-statistics-information>
<clear-dhcp-security-binding>
<clear-dhcp-security-binding-interface>
<clear-dhcp-security-binding-ip-address>
<clear-dhcp-security-binding-statistics>
<clear-dhcp-security-binding-vlan>
clear dhcp relay statistics bulk-leasequery-connections
<clear-dhcp-relay-bulk-leasequery-conn-statistics>
clear dhcp relay statistics leasequery
<clear-dhcp-relay-leasequery-statistics>
clear dhcp server
clear dhcp server binding
<clear-dhcp-server-binding-information>
clear dhcp server binding interface
<clear-dhcp-server-binding-interface>
clear dhcp server statistics
<clear-server-statistics-information>
clear dhcp statistics
<clear-dhcp-service-statistics-information>
clear dhcpv6
clear dhcpv6 proxy-client
clear dhcpv6 proxy-client statistics
<clear-dhcpv6-proxy-client-statistics-information>
clear dhcpv6 relay
clear dhcpv6 relay binding

```

```
clear dhcpv6 relay binding interface
clear dhcpv6 relay statistics
<clear-dhcpv6-relay-statistics-information>
clear dhcpv6 relay statistics bulk-leasequery-connections
<clear-dhcpv6-relay-bulk-leasequery-conn-statistics>
clear dhcpv6 relay statistics leasequery
<clear-dhcpv6-relay-leasequery-statistics>
clear dhcpv6 server
clear dhcpv6 server binding
<clear-dhcpv6-server-binding-information>
clear dhcpv6 server binding interface
<clear-dhcpv6-server-binding-interface>
clear dhcpv6 server statistics
<clear-dhcpv6-server-statistics-information>
clear dhcpv6 server statistics bulk-leasequery-connections
<clear-dhcpv6-server-bulk-leasequery-statistics>
clear dhcpv6 statistics
<clear-dhcpv6-service-statistics-information>
clear diameter
clear diameter function
<clear-diameter-function>
clear diameter peer
<clear-diameter-peer>
<clear-dhcp-binding-information>
<clear-dhcp-conflict-information>
<clear-dhcp-statistics-information>
clear system subscriber-management
clear system subscriber-management statistics
<clear-subscriber-management-statistics>
clear dot1x
clear dot1x firewall
<clear-dot1x-firewall>
clear dot1x firewall interface
<clear-dot1x-firewall-interface>
clear dot1x interface
<clear-dot1x-interface-session>
clear dot1x mac-address
<clear-dot1x-mac-session>
clear dot1x statistics
<clear-dot1x-statistics>
clear dot1x statistics interface
<clear-dot1x-statistics-interface>
clear error
clear error bpdu
clear error bpdu interface
<clear-bpdu-error>
clear error mac-rewrite
clear error mac-rewrite interface
<clear-mac-rewrite-error>
clear esis
clear esis adjacency
<clear-esis-adjacency>
clear esis statistics
<clear-esis-statistics>
clear ethernet-switching
clear ethernet-switching evpn
clear ethernet-switching evpn arp-table
<clear-ethernet-switching-evpn-arp-table>
clear ethernet-switching mac-learning-log
<clear-ethernet-switching-mac-learning-log>
clear ethernet-switching recovery-timeout
```

```

<clear-ethernet-switching-recovery>
clear ethernet-switching recovery-timeout interface
<clear-ethernet-switching-recovery-interface>
clear ethernet-switching table
<clear-ethernet-switching-table>
clear ethernet-switching table interface
<clear-ethernet-switching-interface-table>
clear ethernet-switching table persistent-learning
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning interface
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning mac
<clear-ethernet-switching-table-persistent-learning-mac>
clear evpn
clear evpn arp-table
<clear-evpn-arp-table>
clear evpn mac-table
<clear-evpn-mac-table>
clear evpn mac-table interface
<clear-evpn-interface-mac-table>
clear extensible-subscriber-services
clear extensible-subscriber-services counters
<clear-extensible-subscriber-services-counters>
clear extensible-subscriber-services sessions
<clear-extensible-subscriber-services-sessions>
clear fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-conters>
clear firewall log
<clear-firewall-log>
clear firewall policer
clear firewall policer counter
clear firewall policer counter all
<clear-interface-aggregate-fwd-options>
<clear-interface-aggregate-fwd-options-all>
clear helper
clear helper statistics
<clear-helper-statistics-information>
clear igmp
clear igmp membership
<clear-igmp-membership>
clear igmp snooping
clear igmp snooping membership
<clear-igmp-snooping-membership>
clear igmp snooping membership bridge-domain
<clear-igmp-snooping-bridge-domain-membership>
clear igmp snooping membership vlan
<clear-igmp-snooping-vlan-membership>
clear igmp snooping statistics
<clear-igmp-snooping-statistics>
clear igmp snooping statistics bridge-domain
<clear-igmp-snooping-bridge-domain-statistics>
clear igmp snooping statistics vlan
<clear-igmp-snooping-vlan-statistics>
clear igmp statistics
<clear-igmp-statistics>

```

```
clear ike
clear ike security-associations
<clear-ike-security-associations>
clear ike statistics
<clear-ike-statistics>
clear ilmi
clear ilmi statistics
<clear-ilmi-statistics>
clear interfaces
clear interfaces interface-set
clear interfaces interface-set statistics
<clear-interface-set-statistics>
clear interfaces interface-set statistics all
<clear-interface-set-statistics-all>
clear interfaces interval
<clear-interfaces-interval>
clear interfaces mac-database
<clear-interfaces-mac-database>
clear interfaces mac-database statistics
<clear-interface-mac-database-statistics>
clear interfaces mac-database statistics all
<clear-interface-mac-database-statistics-all>
clear interfaces statistics
<clear-interfaces-statistics>
clear interfaces statistics all
<clear-interfaces-statistics-all>
clear interfaces transport
<clear-interface-transport-information>
clear interfaces transport optics
<clear-interface-transport-optics-information>
clear interfaces transport optics interval
<clear-interface-transport-optics-interval-information>
clear ipsec
clear ipsec security-associations
<clear-ipsec-security-associations>
clear ipv6
clear ipv6 neighbors
<clear-ipv6-nd-information>
clear ipv6 neighbors all
<clear-ipv6-all-neighbors>
clear isis
clear isis adjacency
<clear-isis-adjacency-information>
clear isis database
<clear-isis-database-information>
clear isis overload
<clear-isis-overload-information>
clear isis statistics
<clear-isis-statistics-information>
clear ipv6 router-advertisement
clear lacp
clear lacp statistics
clear l2-learning
clear l2-learning evpn
clear l2-learning evpn arp-statistics
<clear-evpn-arp-statistics>
clear l2-learning evpn arp-statistics interface
<clear-evpn-arp-statistics-interface>
clear l2-learning mac-move-buffer
<clear-l2-learning-mac-move-buffer>
clear l2-learning mac-move-buffer active
```

```
<clear-l2-learning-mac-move-buffer-active>
clear-l2-learning-redundancy-group
<clear-l2-learning-redundancy-group-statistics>
clear l2-learning remote-backbone-edge-bridges
<clear-l2-learning-remote-backbone-edge-bridges>
clear ldp
clear ldp statistics
<clear-ldp-statistics>
clear ldp statistics interface
<clear-ldp-interface-hello-statistics>
clear ldp neighbor
<clear-ldp-neighbors>
clear ldp session
<clear-ldp-sessions>
clear lldp
clear lldp neighbors
<clear-lldp-neighbors>
clear lldp neighbors interface
<clear-lldp-interface-neighbors>
clear lldp statistics
<clear-lldp-statistics>
clear lldp statistics interface
<clear-lldp-interface-statistics>
clear mld
clear mld membership
<clear-mld-membership>
clear mld snooping
clear mld snooping membership
<clear-mld-snooping-membership>
clear mld snooping membership bridge-domain
<clear-mld-snooping-bridge-domain-membership>
clear mld snooping membership vlan
<clear-mld-snooping-vlan-membership>
clear mld snooping statistics
<clear-mld-snooping-statistics>
clear mld snooping statistics bridge-domain
<clear-mld-snooping-bridge-domain-statistics>
clear mld snooping statistics vlan
<clear-mld-snooping-vlan-statistics>
clear mld statistics
<clear-mld-statistics>
clear mobile-ip
clear mobile-ip binding
clear mobile-ip binding all
<clear-binding-all>
clear mobile-ip binding ip-address
<clear-binding-ip>
clear mobile-ip binding nai
<clear-binding-nai>
clear mobile-ip visitor
clear mobile-ip visitor all
<clear-visitor-all>
clear mobile-ip visitor ip-address
<clear-visitor-ip>
clear mobile-ip visitor nai
<clear-visitor-nai>
clear mpls
clear mpls lsp
<clear-mpls-lsp-information>
clear mpls static-lsp
<clear-mpls-static-lsp-information>
```

```
clear mpls traceroute
clear mpls traceroute database
clear mpls traceroute database ldp
<clear-mpls-traceroute-database-ldp>
clear msdp
clear msdp cache
<clear-msdp-cache>
clear msdp statistics
<clear-msdp-statistics>
clear multicast
clear multicast bandwidth-admission
<clear-multicast-bandwidth-admission>
clear multicast forwarding-cache
clear multicast scope
<clear-multicast-scope-statistics>
clear multicast sessions
<clear-multicast-sessions>
clear multicast statistics
<clear-multicast-statistics>
clear mvrp
clear mvrp statistics
<clear-mvrp-interface-statistics>
clear network-access
clear network-access aaa
clear network-access aaa statistics
<clear-aaa-statistics-table>
clear network-access aaa statistics address-assignment
clear network-access aaa statistics address-assignment client
<clear-aaa-address-assignment-client-statistics>
clear network-access aaa statistics address-assignment pool
<clear-aaa-address-assignment-pool-statistics>
clear network-access aaa subscriber
<clear-aaa-subscriber-table>
clear network-access aaa subscriber statistics
<clear-aaa-subscriber-table-specific-statistics>
clear network-access requests
clear network-access requests pending
<clear-authentication-pending-table>
clear network-access requests statistics
<clear-authentication-statistics>
clear network-access securid-node-secret-file
<clear-node-secret-file>
clear oam
clear oam ethernet
clear oam ethernet connectivity-fault-management
clear oam ethernet connectivity-fault-management continuity-measurement
<clear-cfm-continuity-measurement>
clear oam ethernet connectivity-fault-management delay-statistics
<clear-cfm-delay-statistics>
clear oam ethernet connectivity-fault-management event
<clear-cfm-action-profile-event>
clear oam ethernet connectivity-fault-management loss-statistics
<clear-cfm-loss-statistics>
clear oam ethernet connectivity-fault-management path-database
<clear-cfm-linktrace-path-database>
clear oam ethernet connectivity-fault-management policer
<clear-cfm-policer-statistics>
clear oam ethernet connectivity-fault-management sla-iterator-statistics
<clear-cfm-iterator-statistics>
clear oam ethernet connectivity-fault-management statistics
<clear-cfm-statistics>
```

```

clear oam ethernet connectivity-fault-management synthetic-loss-statistics
<clear-cfm-slm-statistics>
clear oam ethernet link-fault-management
clear oam ethernet link-fault-management state
  <clear-lfmd-state>
clear oam ethernet link-fault-management statistics
  <clear-lfmd-statistics>
clear oam ethernet link-fault-management statistics action-profile
  <clear-lfmd-action-profile-statistics>
clear oam ethernet lmi
clear oam ethernet lmi statistics
  <clear-elmi-statistics>
clear ospf
clear ospf database
  <clear-ospf-database-information>
clear ospf database-protection
<clear-ospf-database-protection>
clear ospf io-statistics
  <clear-ospf-io-statistics-information>
clear ospf neighbor
  <clear-ospf-neighbor-information>
clear ospf overload
  <clear-ospf-overload-information>
clear ospf statistics
  <clear-ospf-statistics-information>
clear ospf3
clear ospf3 database
  <clear-ospf3-database-information>
clear ospf3 database-protection
  <clear-ospf3-database-protection>
clear ospf3 io-statistics
  <clear-ospf3-io-statistics-information>
clear ospf3 neighbor
  <clear-ospf3-neighbor-information>
clear ospf3 overload
  <clear-ospf3-overload-information>
clear ospf3 statistics
  <clear-ospf3-io-statistics-information>
clear ovsdb statistics interface all
<clear-ovsdb-interfaces-statistics-all>
clear performance-monitoring
clear performance-monitoring mpls
clear performance-monitoring mpls lsp
<clear-pm-mpls-lsp-information>
clear pfe
clear pfe statistics
clear pfe statistics fabric
clear pfe statistics traffic detail
clear passive-monitoring
  <clear-passive-monitoring>
clear passive-monitoring statistics
  <clear-passive-monitoring-statistics>
clear pgm
clear pgm negative-acknowledgments
  <clear-pgm-negative-acknowledgments>
clear pgm source-path-messages
  <clear-pgm-source-path-messages>
clear pgm statistics
  <clear-pgm-statistics>
clear pim
clear pim join

```

```
<clear-pim-join-state>
clear pim join-distribution
<clear-pim-join-distribution>
clear pim register
<clear-pim-register-state>
clear pim snooping
clear pim snooping join
clear pim snooping statistics
clear pim statistics
<clear-pim-statistics>
clear ppp
clear ppp statistics
<clear-ppp-statistics-information>
clear pppoe
clear pppoe lockout
<clear-pppoe-lockout-timers>
clear pppoe sessions
<clear-pppoe-sessions-information>
clear pppoe statistics
<clear-pppoe-statistics-information>
clear pppoe statistics interfaces
<clear-pppoe-statistics-interface-information>
clear protection-group
<clear-protection-group>
clear protection-group ethernet-ring
<clear-ethernet-ring-information>
clear protection-group ethernet-ring statistics
<clear-ethernet-ring-information>
clear r2cp
clear r2cp radio
<clear-r2cp-radio>
clear r2cp session
<clear-r2cp-session>
clear r2cp statistics
<clear-r2cp-statistics>
clear r2cp statistics radio
clear r2cp statistics session
clear rip
clear rip general-statistics
<clear-rip-general-statistics>
clear rip statistics
<clear-rip-statistics>
clear rip statistics peer
<clear-rip-peer-statistics>
clear ripng
clear ripng general-statistics
<clear-ripng-general-statistic>
clear ripng statistics
<clear-ripng-statistics>
clear rsvp
clear rsvp session
<clear-rsvp-session-information>
clear rsvp statistics
< clear-rsvp-counters-information>
clear security group-vpn
clear security group-vpn member
clear security group-vpn member ike
clear security group-vpn member ike security-associations
<clear-group-vpn-ike-security-associations>
clear security group-vpn member ipsec
clear security group-vpn member ipsec security-associations
```



```

<clear-gvpn-ipsec-security-association>
clear security group-vpn member ipsec security-associations statistics
<clear-gvpn-ipsec-security-association-statistics>
clear security group-vpn member ipsec statistics
<clear-gvpn-ipsec-statistics>
clear services
clear services alg
clear services alg statistics
<clear-services-alg-statistics>
clear services application-aware-access-list
clear services application-aware-access-list statistics
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics interface
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics subscriber
<clear-application-aware-access-list-statistics-subscriber>
clear services application-identification
clear services application-identification application-system-cache
<clear-appid-application-system-cache>
clear services application-identification counter
<clear-appid-counter>
clear services application-identification counter ssl-encrypted-sessions
<clear-appid-counter-encrypted>
clear services application-identification statistics
<clear-appid-application-statistics>
clear services application-identification statistics cumulative
<clear-appid-application-statistics-cumulative>
clear services application-identification statistics interval
<clear-appid-application-statistics-interval>
clear services border-signaling-gateway
clear services border-signaling-gateway denied-messages
<clear-service-bsg-denied-messages>
clear services border-signaling-gateway name-resolution-cache
clear services border-signaling-gateway name-resolution-cache all
<clear-service-border-signaling-gateway-name-resolution-cache-all>
clear services border-signaling-gateway name-resolution-cache by-fqdn
<clear-border-signaling-gateway-name-resolution-cache-by-fqdn>
clear services border-signaling-gateway statistics
<clear-service-border-signaling-gateway-statistics>
clear services captive-portal-content-delivery
clear services captive-portal-content-delivery statistics
clear services captive-portal-content-delivery statistics interface
<clear-cpcdd-interface-statistics>
clear services cos
clear services cos statistics
<clear-services-cos-statistics>
clear services crtp
clear services crtp statistics
<clear-services-crtp-statistics>
clear services dynamic-flow-capture
clear services dynamic-flow-capture criteria
<clear-services-dynamic-flow-capture-criteria>
clear services dynamic-flow-capture sequence-number
clear services flow-collector
<clear-services-flow-collector-information>
clear services flow-collector statistics
<clear-services-flow-collector-statistics>
clear service-msp-flow-ipaction-table
clear services ids
<clear-services-ids-tables>
clear services ids destination-table

```

```
<clear-services-ids-destination-table>
clear services ids pair-table
<clear-services-ids-pair-table>
clear services ids source-table
<clear-services-ids-source-table>
clear services inline
clear services inline nat
clear services inline nat pool
<clear-inline-nat-pool-information>
clear services inline nat statistics
<clear-inline-nat-statistics>
clear services inline softwire
clear services inline softwire statistics
<clear-inline-softwire-statistics>
clear services ipsec-vpn
clear services ipsec-vpn ipsec
clear services ipsec-vpn ipsec security-associations
<clear-services-ipsec-vpn-security-associations>
clear services ipsec-vpn ike
clear services ipsec-vpn ike security-associations
<clear-services-ike-security-associations>
clear services ipsec-vpn ike statistics
<clear-services-ike-statistics>
clear services pcp
clear services pcp epoch
clear services pcp statistics
clear services ipsec-vpn ipsec statistics
<clear-ipsec-vpn-statistics>
clear services l2tp
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp multilink
<clear-l2tp-multilink-information>
clear services l2tp session
<clear-l2tp-session-information>
clear services l2tp destination
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp tunnel
<clear-l2tp-tunnel-information>
clear services l2tp user
<clear-l2tp-user-session-information>
clear services local-policy-decision-function
clear services local-policy-decision-function statistics
clear services local-policy-decision-function statistics interface
<clear-local-policy-decision-function-statistics-interface>
clear services local-policy-decision-function statistics subscriber
<clear-local-policy-decision-function-statistics-subscriber>
clear services server-load-balance
  clear services server-load-balance external-manager-statistics
<clear-external-manager-statistics>
clear services server-load-balance hash-table
<clear-hash-table-information>
clear services server-load-balance health-monitor-statistics>
<clear-health-monitor-statistics>
clear services server-load-balance real-server-group-statistics
<clear-real-server-group-statistics>
clear services server-load-balance real-server-statistics
<clear-real-server-statistics>
```

```
clear services server-load-balance sticky
<clear-sticky-table>
clear services server-load-balance virtual-server-statistics>
<clear-virtual-server-statistics>
clear services service-sets statistics integrity-drops
clear services service-sets statistics syslog
<clear-service-set-syslog-statistics>
clear services stateful-firewall flow-analysis
<clear-service-flow-analysis>
clear services stateful-firewall flows
<clear-service-sfw-flow-table-information>
clear services stateful-firewall sip-call
<clear-service-sfw-sip-call-information>
clear services stateful-firewall sip-register
<clear-service-sfw-sip-register-information>
clear services stateful-firewall statistics
<clear-stateful-firewall-statistics>
clear services stateful-firewall subscriber-analysis
<clear-service-subs-analysis>
clear services subscriber
clear services subscriber sessions
<get-services-subscriber-sessions>
clear services video-monitoring
<clear-service-video-monitoring-information>
clear services video-monitoring mdi
<clear-service-video-monitoring-mdi-information>
clear services video-monitoring mdi alarm
<clear-service-video-monitoring-mdi-alarm-information>
clear services video-monitoring mdi alarm errors
<clear-services-video-monitoring-mdi-alarm-errors>
clear services video-monitoring mdi alarm stats
<clear-services-video-monitoring-mdi-alarm-statistics>
clear services video-monitoring mdi errors
<clear-service-video-monitoring-mdi-errors>
clear services video-monitoring mdi statistics
<clear-service-video-monitoring-mdi-statistics>
clear services softwire
clear services softwire statistics
<clear-services-softwire-statistics>
clear services stateful-firewall
clear services stateful-firewall flow-analysis
<clear-service-flow-analysis>
clear services stateful-firewall flows
<clear-service-sfw-flow-table-information>
clear services pgcp
clear services pgcp gates
<clear-service-pgcp-gates>
clear services pgcp gates gateway
<clear-service-pgcp-gates-gateway>
clear services pgcp statistics
<clear-service-pgcp-statistics>
clear services pgcp statistics gateway
<clear-service-pgcp-statistics-gateway>
<clear-rfc2544-information>
<clear-aborted-tests-information>
<clear-active-tests-information>
<clear-completed-tests-information>
clear sflow
clear sflow collector
clear sflow collector statistics
<clear-sflow-collector-statistics>
```

```
clear snmp
clear snmp history
<clear-snmp-history>
clear snmp statistics
<clear-snmp-statistics>
clear spanning-tree
clear spanning-tree protocol-migration
clear spanning-tree protocol-migration interface
<clear-interface-stp-protocol-migration>
clear spanning-tree statistics
<clear-stp-interface-statistics>
clear spanning-tree statistics bridge
clear spanning-tree statistics interface
clear spanning-tree statistics routing-instance
<clear-stp-routing-instance-statistics>
clear spanning-tree stp-buffer
clear spanning-tree topology-change-counter
<clear-stp-topology-change-counter>
clear synchronous-ethernet
clear synchronous-ethernet esmc
clear synchronous-ethernet esmc statistics
clear system
clear system boot-media
<clear-boot-media>
clear system login
  clear system login logout
<clear-system-login-logout>
clear-twamp-information
clear-twamp-server-information
clear-twamp-server-connection-information
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
```

```
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
```

```
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear validation
clear validation database
<clear-validation-database>
clear validation session
<clear-validation-session>
clear validation statistics
<clear-validation-statistics>
clear virtual-chassis
clear virtual-chassis heartbeat
<clear-virtual-chassis-heartbeat-statistics>
<clear-virtual-chassis-protocol>
clear virtual-chassis protocol statistics
<clear-virtual-chassis-statistics>
<clear-virtual-chassis-port-statistics>
clear vpls
clear vpls mac-address
<clear-vpls-mac-address>
clear vpls mac-table
<clear-vpls-mac-table>
clear vpls mac-table interface
<clear-vpls-interface-mac-table>
request interface rebalance
request pppoe
request pppoe connect
request pppoe disconnect
request security ike debug-disable
<get-disable-ike-debug>
request security ike debug-enable
<get-enable-ike-debug>
request services rpm twamp start
request services rpm twamp start client
<twamp-test-start>
request services rpm twamp stop
request services rpm twamp stop client
<twamp-test-stop>
request snmp
<request-snmp-utility-mib-clear>
<request-snmp-utility-mib-set>
clear vpls statistics
<clear-vpls-statistics>
clear vrrp
<clear-vrrp-information>
clear vrrp interface
<clear-vrrp-interface-statistics>
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
clear services inline stateful-firewall
clear services inline stateful-firewall flows
<clear-service-inline-sfw-flow-table-information>
clear services inline stateful-firewall statistics
<clear-inline-stateful-firewall-statistics>
clear services service-sets statistics drop-flow-limit>
```

```

<clear-service-set-drop-flow-statistics>
clear services service-sets statistics jflow-log
<clear-service-set-jflow-log-statistics>
request services ipsec-vpn ipsec
request services ipsec-vpn ipsec switch
request services ipsec-vpn ipsec switch tunnel
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>

```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

configure

Can enter configuration mode.

Commands

```

configure
request snmp
request-snmp-utility-mib-clear
request-snmp-utility-mib-set

```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)

- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

control

Can perform all control-level operations; can modify any configuration.

Commands	<code>request jnu</code> <code>request jnu role</code> <code>request jnu schema</code> <code>request jnu schema add</code> <code>request jnu schema delete</code>
----------	---

Configuration Hierarchy Levels	No associated CLI configuration hierarchy levels and statements.
--------------------------------	--

- | | |
|-----------------------|---|
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 840• Understanding Junos OS Access Privilege Levels on page 799• Configuring Access Privilege Levels on page 829• Specifying Access Privileges for Junos OS Operational Mode Commands on page 830• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834 |
|-----------------------|---|

field

Can view field debug commands.

Commands	No associated CLI commands.
----------	-----------------------------

Configuration Hierarchy Levels	No associated CLI configuration hierarchy levels and statements.
--------------------------------	--

- | | |
|-----------------------|---|
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 840• Understanding Junos OS Access Privilege Levels on page 799• Configuring Access Privilege Levels on page 829• Specifying Access Privileges for Junos OS Operational Mode Commands on page 830• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834 |
|-----------------------|---|

firewall

Can view the firewall filter configuration in configuration mode.

Commands	<pre>show firewall <get-firewall-information> show firewall counter <get-firewall-counter-information> show firewall filter <get-firewall-filter-information> show firewall filter version <get-filter-version> show firewall log <get-firewall-log-information> show firewall prefix-action-stats <get-firewall-prefix-action-information> show policer <get-policer-information></pre>
Configuration Hierarchy Levels	<pre>[edit dynamic-profiles firewall] [edit firewall] [edit logical-systems firewall]</pre>
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 830 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834 • firewall-control on page 897

firewall-control

Can view and configure firewall filter information at the `[edit dynamic-profiles firewall]`, `[edit firewall]`, and `[edit logical-systems firewall]` hierarchy levels.

Commands	<pre>show firewall <get-firewall-information> show firewall counter <get-firewall-counter-information> show firewall filter <get-firewall-filter-information> show firewall filter version <get-filter-version> show firewall log <get-firewall-log-information> show firewall prefix-action-stats <get-firewall-prefix-action-information></pre>
-----------------	--

	<code>show policer</code>
Configuration Hierarchy Levels	<code>[edit dynamic-profiles firewall]</code> <code>[edit firewall]</code> <code>[edit logical-systems firewall]</code>
Related Documentation	<ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 840• Understanding Junos OS Access Privilege Levels on page 799• Configuring Access Privilege Levels on page 829• Specifying Access Privileges for Junos OS Operational Mode Commands on page 830• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834• firewall on page 896

floppy

	Can read from and write to the removable media.
Commands	No associated CLI commands.
Configuration Hierarchy Levels	No associated CLI configuration hierarchy levels and statements.
Related Documentation	<ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 840• Understanding Junos OS Access Privilege Levels on page 799• Configuring Access Privilege Levels on page 829• Specifying Access Privileges for Junos OS Operational Mode Commands on page 830• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834

flow-tap

	Can view the flow-tap configuration in configuration mode.
Commands	No associated CLI commands.
Configuration Hierarchy Levels	<code>[edit services flow-tap]</code> <code>[edit services radius-flow-tap]</code> <code>[edit system services flow-tap-dtcp]</code>
Related Documentation	<ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 840• Understanding Junos OS Access Privilege Levels on page 799• Configuring Access Privilege Levels on page 829• Specifying Access Privileges for Junos OS Operational Mode Commands on page 830

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [flow-tap-control on page 899](#)

flow-tap-control

Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the **[edit services flow-tap]**, **[edit services radius-flow-tap]**, and **[edit system services flow-tap-dtcp]** hierarchy levels.

Commands No associated CLI commands.

Configuration Hierarchy Levels

- `[edit services flow-tap]`
- `[edit services radius-flow-tap]`
- `[edit system services flow-tap-dtcp]`

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [flow-tap on page 898](#)

flow-tap-operation

Can make flow-tap requests to the router.

Commands No associated CLI commands.

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

idp-profiler-operation

Can view profiler data.

Commands No associated CLI commands.

CLI Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

interface

Can view the interface configuration in configuration mode.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit accounting-options]
[edit chassis]
[edit class-of-service]
[edit class-of-service interfaces]
[edit dynamic-profiles class-of-service]
[edit dynamic-profiles class-of-service interfaces]
[edit dynamic-profiles interfaces]
[edit dynamic-profiles routing-instances instance system services
dhcp-local-server]
[edit dynamic-profiles routing-instances instance system services
static-subscribers group]
[edit forwarding-options]
[edit interfaces]
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services
dhcp-local-server]
[edit logical-systems routing-instances instance system services
static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
[edit services radius-flow-tap interfaces]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
 - [interface-control on page 901](#)

interface-control

Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the **[edit chassis]**, **[edit class-of-service]**, **[edit groups]**, **[edit forwarding-options]**, and **[edit interfaces]** hierarchy levels.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit accounting-options]
[edit chassis]
[edit class-of-service]
[edit class-of-service interfaces]
[edit dynamic-profiles class-of-service]
[edit dynamic-profiles class-of-service interfaces]
[edit dynamic-profiles interfaces]
[edit dynamic-profiles routing-instances instance system services
dhcp-local-server]
[edit dynamic-profiles routing-instances instance system services
static-subscribers group]
[edit forwarding-options]
[edit interfaces]
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services
dhcp-local-server]
[edit logical-systems routing-instances instance system services
static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
[edit services radius-flow-tap interfaces]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
 - [interface on page 900](#)

maintenance

Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell, and can halt and reboot the router.

Commands	<pre>clear system reboot <clear-reboot> clear-system-services-reverse-information file archive <file-archive> file change-owner <file-change-owner> <extract-file> monitor traffic request chassis afeb request chassis beacon <request-chassis-beacon> request chassis cb <request-chassis-cb> request chassis ccg <request-chassis-ccg> request chassis cfeb request chassis cfeb master request chassis cip request chassis fabric request chassis fabric device request chassis fabric guided-cabling request chassis fabric plane request chassis fabric upgrade-bandwidth request chassis fabric upgrade-bandwidth fpc request chassis fabric upgrade-bandwidth info request chassis feb <request-feb> request chassis fpc <request-chassis-fpc> request chassis mcs request chassis mic request chassis optics request chassis pcg request chassis pic <request-chassis-pic> request chassis redundancy request chassis redundancy feb <request-redundancy-feb> request chassis routing-engine <request-chassis-routing-engine> request chassis routing-engine hard-disk-test request chassis routing-engine master request chassis scg request chassis sfb request chassis sfm request chassis sfm master request chassis sib <request-chassis-sib> request chassis sib f13 request chassis sib f2s request chassis sib optics request chassis spmb <request-chassis-spmb> request chassis ssb request chassis ssb master request chassis synchronization</pre>
-----------------	---

```

request chassis synchronization force
request chassis synchronization force automatic-switching
request chassis synchronization force mark-failed
request chassis synchronization force unmark-failed
request chassis synchronization switch
request chassis tfep
request chassis vcpu
request chassis vnpu
request diagnostics
request diagnostics tdr
request diagnostics tdr abort
request diagnostics tdr abort interface
<abort-tdr-interface-diagnostics>
request diagnostics tdr start
request diagnostics tdr start interface
<request-tdr-interface-diagnostics>
request l2circuit-switchover
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
    <reload-eedebg-action-profile>

request security idp
    <request-idp-security-policy-load>

request security idp security-package
request security idp security-package download
    <request-idp-security-package-download>

request security idp security-package download version
    <request-idp-security-package-download-version>

request security idp security-package install
    <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
    <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
    <request-idp-ssl-key-delete>
request security idp storage-cleanup
    <request-idp-storage-cleanup>
request security ike
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate ca-profile-group
request security pki ca-certificate ca-profile-group load
request security pki ca-certificate enroll
request security pki local-certificate export
request security pki ca-certificate load
    <load-pki-ca-certificate>

```

```
request security pki ca-certificate verify
    <verify-pki-ca-certificate>
request security pki crl
request security pki crl load
    <load-pki-crl>
request security pki generate-certificate-request
    <generate-pki-certificate-request>
request security pki generate-key-pair
    <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
    <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
    <load-pki-local-certificate>
request security pki local-certificate verify
    <verify-pki-local-certificate>
request security pki verify-integrity-status
<verify-integrity-status>
request services fips
request services fips authorize
request services fips authorize pic
request services fips zeroize
request services fips zeroize pic
request services flow-collector
request services flow-collector change-destination
    <request-services-flow-collector-destination>

request services ggsn
request services ggsn pdp
request services ggsn pdp terminate
request services ggsn pdp terminate apn
    <request-ggsn-terminate-contexts-apn>

request services ggsn pdp terminate context
    <request-ggsn-terminate-context>

request services ggsn pdp terminate context msisdn
    <request-ggsn-terminate-msisdn-context>

request services ggsn restart
request services ggsn restart interface
    <request-ggsn-restart-interface>

request services ggsn restart node
    <request-ggsn-restart-node>

request services ggsn start
request services ggsn start interface
request services ggsn stop
request services ggsn stop interface
    <request-ggsn-stop-interface>

request services ggsn stop node
    <request-ggsn-stop-node>

request services ggsn trace
request services ggsn trace software
request services ggsn trace software update
    <request-ggsn-software-update>
```



```
request services ggsn trace start
request services ggsn trace start imsi
    <request-ggsn-start-imsi-trace>

request services ggsn trace start msisdn
    <request-ggsn-start-msisdn-trace>

request services ggsn trace stop
request services ggsn trace stop all
    <request-ggsn-stop-trace-activity>

request services ggsn trace stop imsi
    <request-ggsn-stop-imsi-trace>

request services ggsn trace stop msisdn
    <request-ggsn-stop-msisdn-trace>

request support
request support information
request system
request system boot-media
<request-boot-media>
request system certificate
request system certificate add
request system commit
request system commit server
request system commit server pause
<request-commit-server-pause>
request system commit server queue
request system commit server queue cleanup
<request-commit-server-cleanup>
request system commit server start
<request-commit-server-start>
request system configuration
request system configuration rescue
request system configuration rescue delete
    <request-delete-rescue-configuration>

request system configuration rescue save
    <request-save-rescue-configuration>
request system diagnostics
request system diagnostics log-archive
<request-log>
request system diagnostics transfer-control
<transfer-control>
request system firmware
request system firmware downgrade
request system firmware downgrade feb
request system firmware downgrade fpc
request system firmware downgrade pic
request system firmware downgrade poe
request system firmware downgrade re
request system firmware downgrade scb
request system firmware downgrade sfm
request system firmware downgrade spmb
request system firmware downgrade ssb
request system firmware downgrade vcpu
request system firmware upgrade
request system firmware upgrade feb
request system firmware upgrade fpc
request system firmware upgrade fpga
```

```
request system firmware upgrade fpga fpc
request system firmware upgrade fpga scb
<request-scb-fpga-upgrade>
request system firmware upgrade pic
request system firmware upgrade poe
request system firmware upgrade re
request system firmware upgrade re bios
request system firmware upgrade scb
request system firmware upgrade sfm
request system firmware upgrade spmb
request system firmware upgrade ssb
request system firmware upgrade vcpu
request system halt
  <request-halt>

request system keep-alive
request system license
request system license add
request system license delete
  <request-license-delete>
request system license revoke-licenses
<license-revoke-licenses>

request system license save
request system license update
  <request-license-update>
request system logout
request system partition
request system partition abort
request system partition compact-flash
request system partition hard-disk
request system power-off
  <request-power-off>

request system power-on
<request-power-on-other-re>
request system process
request system process terminate
<request-process-terminate>
request system reboot
  <request-reboot>
request system recover

request system scripts
request system scripts add
  <request-scripts-package-add>

request system scripts convert
request system scripts convert slax-to-xslt
request system scripts convert xslt-to-slax
request system scripts delete
  <request-scripts-package-delete>

request system scripts event-scripts
request system scripts event-scripts reload
  <reload-event-scripts>

request system scripts refresh-from
  <request-script-refresh-from>

request system scripts rollback
```

```

    <request-scripts-package-rollback>

request system scripts synchronize
<request-scripts-synchronize>

request system snapshot
    <request-snapshot>

request system software
request system software abort
request system software abort in-service-upgrade
    <abort-in-service-upgrade>

request system software add
    <request-package-add>

request system software delete
    <request-package-delete>

request system software delete-backup
    <request-package-delete-backup>

request system software in-service-upgrade
    <request-package-in-service-upgrade>

request system software nonstop-upgrade
    <request-package-nonstop-upgrade>
request system software recovery-package
request system software recovery-package add
request system software recovery-package delete
request system software recovery-package extract
request system software recovery-package extract ex-8200-package
request system software recovery-package extract ex-xre200-package
request system software rollback
    <request-package-rollback>

request system software validate
    <request-package-validate>
request system software validate in-service-upgrade
    <check-in-service-upgrade>

request system storage
request system storage cleanup
    <request-system-storage-cleanup>
request system storage cleanup qfabric
    <remove-qfabric-repository-contents>
request system storage mount
<request-mount>
request system storage unified-edge
request system storage unified-edge charging
request system storage unified-edge charging media
request system storage unified-edge media
request system storage unified-edge media eject
request system storage unified-edge media prepare
request system storage unmount
<request-unmount>
request system subscriber-management
request system subscriber-management new-sessions-disable
<request-sm-new-sessions-disable>
request system subscriber-management new-sessions-enable
<request-sm-new-sessions-enable>

```

```
request system zeroize
request vpls-switchover
set date
set date ntp
show chassis usb
show chassis usb storage
<get-usb-storage-status>
show services fips
show system configuration database
show system configuration database usage
<get-database-usage>
start shell
start shell user
test access
test access profile
    <get-radius-profile-access-test-result>

test access radius-server
    <get-radius-server-access-test-result>
get-test-services-l2tp-tunnel-result
```

Configuration Hierarchy Levels

```
[edit event-options]
[edit security ipsec internal]
[edit security ipsec trusted-channel]
[edit services dynamic-flow-capture traceoptions]
[edit services ggsn]
[edit system fips]
[edit services ggsn rule-space]
[edit system processes daemon-process command]
[edit system scripts]
[edit system scripts commit]
[edit system scripts op]
[edit system scripts snmp]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

network

Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.

Commands

```
mtrace
mtrace from-source
mtrace monitor
mtrace to-gateway
ping
    <ping>

ping atm
ping clns
```

```
ping ethernet
    <request-ping-ethernet>
ping fibre-channel
ping mpls
ping mpls bgp
    <request-ping-bgp-lsp>
ping mpls l2circuit
ping mpls l2circuit interface
    <request-ping-l2circuit-interface>

ping mpls l2circuit virtual-circuit
    <request-ping-l2circuit-virtual-circuit>

ping mpls l2vpn
ping mpls l2vpn fec129
ping mpls l2vpn fec129 interface
    <request-ping-l2vpn-fec129-interface>
ping mpls l2vpn instance
    <request-ping-l2vpn-instance>

ping mpls l2vpn interface
    <request-ping-l2vpn-interface>

ping mpls l3vpn
    <request-ping-l3vpn>

ping mpls ldp
    <request-ping-ldp-lsp>

ping mpls ldp p2mp
    <request-ping-ldp-p2mp-lsp>

ping mpls lsp-end-point
    <request-ping-lsp-end-point>

ping mpls rsvp
    <request-ping-rsvp-lsp>

ping overlay
    <request-ping-overlay>
ping vpls
ping vpls instance
    <request-ping-vpls-instance>

request routing-engine
request routing-engine login
    <request-routing-engine-login>
request routing-engine login other-routing-engine
    <request-login-to-other-routing-engine>
request services flow-collector
request services flow-collector test-file-transfer
    <request-services-flow-collector-test-file-transfer>

show host
show interfaces level-extra descriptions
show multicast minfo
ssh
telnet
traceroute
    <traceroute>
```

```
traceroute clns
traceroute ethernet
  <request-traceroute-ethernet>
```

```
traceroute monitor
traceroute mpls
traceroute mpls l2vpn
<traceroute-mpls-l2vpn>
traceroute mpls l2vpn fec129
<traceroute-mpls-mspw>
traceroute mpls ldp
<traceroute-mpls-ldp>
traceroute mpls rsvp
<traceroute-mpls-rsvp>
traceroute overlay
<request-traceroute-overlay>
```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

pgcp-session-mirroring

Can view session mirroring configuration by using the **pgcp** command.

Commands `show services pgcp gates gate-way display session-mirroring`

Configuration Hierarchy Levels `[edit services pgcp gateway session-mirroring]`
`[edit services pgcp session-mirroring]`

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
 - [pgcp-session-mirroring-control on page 910](#)

pgcp-session-mirroring-control

Can modify PGCP session mirroring configuration

Commands `show services pgcp gates gate-way display session-mirroring`

Configuration Hierarchy Levels	<pre>[edit services pgcp gateway session-mirroring] [edit services pgcp session-mirroring]</pre>
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 830 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834 • pgcp-session-mirroring on page 910

reset

Can restart software processes by using the **restart** command and can configure whether software processes configured at the **[edit system processes]** hierarchy level are enabled or disabled.

Commands	<pre>request chassis cfeb master switch request chassis cfeb master switch no-confirm request chassis routing-engine master acquire request chassis routing-engine master acquire force request chassis routing-engine master acquire force no-confirm request chassis routing-engine master acquire no-confirm request chassis routing-engine master release request chassis routing-engine master release no-confirm request chassis routing-engine master switch request chassis routing-engine master switch no-confirm request chassis sfm master switch request chassis sfm master switch no-confirm request chassis ssb master switch request chassis ssb master switch no-confirm restart restart kernel-replication <restart-kernel-replication> restart-named-service restart routing <routing-restart> restart services restart services border-signaling-gateway <restart-border-signaling-gateway-service> restart services pgcp <restart-pgcp-service> restart web-management <restart-web-management></pre>
-----------------	--

Configuration Hierarchy Levels	No associated CLI configuration hierarchy levels and statements.
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

rollback

Can roll back to previous configurations.

Commands `rollback`

**Configuration
Hierarchy Levels** `[edit]`

- Related
Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

secret

Can view passwords and other authentication keys in the configuration.

Commands No associated CLI commands.

**Configuration
Hierarchy Levels**

```
[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius-disconnect preauthentication-secret]
[edit access radius-disconnect secret]
[edit access radius-server preauthentication-secret]
[edit access radius-server secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
[edit dynamic-profiles interfaces interface unit ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap
default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap]
[edit logical-systems interfaces interface unit ppp-options pap
default-password]
```



```
[edit logical-systems interfaces interface unit ppp-options pap local-password]
[edit logical-systems routing-instances instance system services
static-subscribers authentication password]
[edit logical-systems routing-instances instance system services
static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication
password]
[edit logical-systems system services static-subscribers group authentication
password]
[edit routing-instances instance system services static-subscribers
authentication password]
[edit routing-instances instance system services static-subscribers group
authentication password]
[edit services ggsn apn radius accounting server secret]
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server preauthentication-secret]
[edit system accounting destination radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server preauthentication-secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius
accounting-shared-secret]
[edit system services static-subscribers authentication password]
[edit system services static-subscribers group authentication password]
[edit system tacplus-server secret]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [secret-control on page 913](#)

secret-control

Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius-disconnect secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
```

```
[edit dynamic-profiles interfaces interface unit ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap
default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap
default-password]
[edit logical-systems interfaces interface unit ppp-options pap local-password]
[edit logical-systems routing-instances instance system services
static-subscribers authentication password]
[edit logical-systems routing-instances instance system services
static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication
password]
[edit logical-systems system services static-subscribers group authentication
password]
[edit routing-instances instance system services static-subscribers
authentication password]
[edit routing-instances instance system services static-subscribers group
authentication password]
[edit services ggsn apn radius accounting server secret]
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius
accounting-shared-secret]
[edit system services static-subscribers authentication password]
[edit system services static-subscribers group authentication password]
[edit system tacplus-server secret]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [secret on page 912](#)

security

Can view security configuration.

Commands

```
clear security
clear security alarms
  <clear-security-alarm-information>
```

```
clear security idp
clear security idp application-ddos
clear security idp application-ddos cache
    <clear-idp-appddos-cache>

clear security idp application-identification
clear security idp application-identification application-system-cache
    <clear-idp-application-system-cache>

clear security idp application-statistics
    <clear-idp-applications-information>

clear security idp attack
clear security idp attack table
    <clear-idp-attack-table>

clear security idp counters
    <clear-idp-counters-by-counter-class>

clear security idp ssl-inspection
clear security idp ssl-inspection session-id-cache
    <clear-idp-ssl-session-cache-information>
clear security idp status
    <clear-idp-status-information>
clear security log
    <clear-security-log-information>
clear security pki
clear security pki ca-certificate
    <clear-pki-ca-certificate>
clear security pki certificate-request
    <clear-pki-certificate-request>
clear security pki crl
    <clear-pki-crl>
clear security pki key-pair
    <clear-pki-key-pair>
clear security pki local-certificate
    <clear-pki-local-certificate>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
    <request-idp-policy-load>
request security idp security-package
request security idp security-package download
    <request-idp-security-package-download>

request security idp security-package download version
    <request-idp-security-package-download-version>

request security idp security-package install
    <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
    <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
```

```
<request-idp-ssl-key-delete>
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
  <load-pki-ca-certificate>
request security pki crl
request security pki crl load
  <request security pki crl load>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki verify-integrity-status
<verify-integrity-status>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
  <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
  <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
  <get-idp-application-system-cache>

show security idp application-statistics
  <get-idp-applications-information>

show security idp attack
show security idp attack description
  <get-idp-attack-description-information>
show security idp attack detail
  <get-idp-attack-detail-information>
show security idp attack table
  <get-idp-attack-table-information>

show security idp counters
  <get-idp-counter-information>

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
  <get-idp-memory-information>

show security idp policies
```

```

<get-idp-subscriber-policy-list>

show security idp policy-templates-list
  <get-idp-policy-template-information>
  <get-idp-predefined-attack-groups>
  <get-idp-predefined-attack-group-filters>
  <get-idp-predefined-attacks>
  <get-idp-predefined-attack-filters>
  <get-idp-recent-security-package-information>
show security idp policy-commit-status
  <get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp security-package-version
  <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
  <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>

```

**Configuration
Hierarchy Levels**

```

[edit security]
[edit security alarms]
[edit security log]

```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [security-control on page 918](#)

security-control

Can view and configure security information at the **[edit security]** hierarchy level.

Commands

```
clear security
clear security alarms
  <clear-security-alarm-information>
clear security idp
clear security idp application-ddos
clear security idp application-ddos cache
  <clear-idp-appddos-cache>

clear security idp application-identification
clear security idp application-identification application-system-cache
  <clear-idp-application-system-cache>

clear security idp application-statistics
  <clear-idp-applications-information>

clear security idp attack
clear security idp attack table
  <clear-idp-attack-table>

clear security idp counters
  <clear-idp-counters-by-counter-class>

clear security idp ssl-inspection
clear security idp ssl-inspection session-id-cache
  <clear-idp-ssl-session-cache-information>
clear security idp status
  <clear-idp-status-information>
clear security log
  <clear-security-log-information>
clear security pki
clear security pki ca-certificate
  <clear-pki-ca-certificate>
clear security pki certificate-request
  <clear-pki-certificate-request>
clear security pki crl
  <clear-pki-crl>
clear security pki key-pair
  <clear-pki-key-pair>
clear security pki local-certificate
  <clear-pki-local-certificate>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
  <request-idp-policy-load>
request security idp security-package
request security idp security-package download
  <request-idp-security-package-download>

request security idp security-package download version
  <request-idp-security-package-download-version>
```

```

request security idp security-package install
  <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
  <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
  <request-idp-ssl-key-delete>
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
  <load-pki-ca-certificate>
request security pki crl
request security pki crl load
  <request security pki crl load>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
  <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
  <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
  <get-idp-application-system-cache>

show security idp application-statistics
  <get-idp-applications-information>

show security idp attack
show security idp attack description
  <get-idp-attack-description-information>
show security idp attack detail
  <get-idp-attack-detail-information>
show security idp attack table
  <get-idp-attack-table-information>

show security idp counters
  <get-idp-counter-information>

```

```
show security idp logical-system
show security idp logical-system policy-association
show security idp memory
  <get-idp-memory-information>

show security idp policies
  <get-idp-subscriber-policy-list>

show security idp policy-templates-list
  <get-idp-policy-template-information>
  <get-idp-predefined-attack-groups>
  <get-idp-predefined-attack-group-filters>
  <get-idp-predefined-attacks>
  <get-idp-predefined-attack-filters>
  <get-idp-recent-security-package-information>
show security idp policy-commit-status
  <get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp security-package-version
  <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
  <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>
```

**Configuration
Hierarchy Levels**

```
[edit security]
[edit security alarms]
[edit security log]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [security on page 914](#)

shell

Can start a local shell on the router.

Commands	<pre>start shell start shell user</pre>
Configuration Hierarchy Levels	No associated CLI configuration hierarchy levels and statements.
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 830 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834

snmp

Can view Simple Network Management Protocol (SNMP) configuration.

Commands	No associated CLI commands.
Configuration Hierarchy Levels	[edit snmp]
Related Documentation	<ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 840 • Understanding Junos OS Access Privilege Levels on page 799 • Configuring Access Privilege Levels on page 829 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 830 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834

system

Can view system-level configuration information.

Commands	<pre>request chassis synchronization request chassis synchronization force request chassis synchronization force automatic-switching request chassis synchronization force mark-failed request chassis synchronization force unmark-failed request chassis synchronization switch</pre>
-----------------	---

```

request virtual-chassis
request virtual-chassis device-reachability
<get-virtual-chassis-diagnostic-information>
request virtual-chassis member-id
request virtual-chassis member-id delete
delete-virtual-chassis-member-id
request virtual-chassis member-id set
<set-virtual-chassis-member-id>
request virtual-chassis mode
request virtual-chassis mode mixed
<request-virtual-chassis-mode-mixed>
request virtual-chassis reactivate
<request-virtual-chassis-reactivate>
request virtual-chassis recycle
<request-virtual-chassis-recycle>
request virtual-chassis renumber
<request-virtual-chassis-renumber>
request virtual-chassis routing-engine
request virtual-chassis routing-engine master
request virtual-chassis routing-engine master switch
<switch-vc-routing-engine-protocol-master>
request virtual-chassis vc-port
request virtual-chassis vc-port delete
request virtual-chassis vc-port delete fpc-slot
<request-virtual-chassis-vc-port-delete-fpc-slot>
request virtual-chassis vc-port delete pic-slot
<request-virtual-chassis-vc-port-delete-pic-slot>
request virtual-chassis vc-port set
request virtual-chassis vc-port set fpc-slot
<request-virtual-chassis-vc-port-set-fpc-slot>
request virtual-chassis vc-port set interface
<request-virtual-chassis-vc-port-set-interface>
request virtual-chassis vc-port set pic-slot
<request-virtual-chassis-vc-port-set-pic-slot>
<set-virtual-chassis-mode>

```

Configuration Hierarchy Levels

```

[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers
  tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit fabric virtual-chassis]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems protocols uplink-failure-detection]
[edit logical-systems routing-instances instance forwarding-options helpers
  bootp]
[edit logical-systems routing-instances instance forwarding-options helpers
  domain]
[edit logical-systems routing-instances instance forwarding-options helpers
  port]
[edit logical-systems routing-instances instance forwarding-options helpers
  tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]

```

```
[edit logical-systems system syslog]
[edit poe]
[edit protocols uplink-failure-detection]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system boot loader authentication]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system no-debugger-on-alt-break]
[edit system no-redirects-ipv6]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports auxiliary silent-with-modem]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system ports console silent-with-modem]
[edit system processes]
[edit system proxy]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
```

```
[edit virtual-chassis locality-bias]
[edit vlans]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [system-control on page 924](#)

system-control

Can view system-level configuration information and configure it at the **[edit system]** hierarchy level.

**Configuration
Hierarchy Levels**

```
[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers
  tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems routing-instances instance forwarding-options helpers
  bootp]
[edit logical-systems routing-instances instance forwarding-options helpers
  domain]
[edit logical-systems routing-instances instance forwarding-options helpers
  port]
[edit logical-systems routing-instances instance forwarding-options helpers
  tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit poe]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
```

```

[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system processes]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
[edit vlans]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [system on page 921](#)

trace

Can view trace file settings and configure trace file properties.

Commands

```

clear log
  <clear-log>
monitor
  request-monitor-ethernet-delay-measurement
  <request-monitor-ethernet-loss-measurement>

```

```

monitor interface
monitor interface traffic
monitor label-switched-path
monitor list
monitor start
monitor static-lsp
monitor stop
show log
<get-log>
show log user
<get-syslog-events>

```

Configuration Hierarchy Levels

```

[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit class-of-service application-traffic-control traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles class-of-service application-traffic-control
traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management
traceoptions]
[dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols oam gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping
traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]

```

```
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery
  traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[edit dynamic-profiles routing-instances instance routing-options multicast
  traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance services mobile-ip
  traceoptions]
[edit dynamic-profiles routing-instances instance system services
  dhcp-local-server traceoptions]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options traceoptions]
[edit jnx-example traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay
  interface-traceoptions]
[edit logical-systems vlans domain multicast-snooping-options traceoptions]
[edit logical-systems vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems forwarding-options dhcp-relay traceoptions]
[edit logical-systems protocols ancp traceoptions]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dot1x traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols ilmi traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols lacp traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet fnp traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam
  traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam
  traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet fnp traceoptions]
[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
```

```
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp lsp-set traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group
traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp group
traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery
traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast
traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip
traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server interface-traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
```



```
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols protocols oam ethernet fnp]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp lsp-set traceoptions]
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
```

```

[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit services l2tp traceoptions]
[edit services server-load-balance traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system ddos-protection traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes dhcp-service interface-traceoptions]
[edit system processes dhcp-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes mag-service traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [trace-control on page 930](#)

trace-control

Can modify trace file settings and configure trace file properties.

Configuration Hierarchy Levels

```

[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]

```

```
[edit vlans domain protocols igmp-snooping traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management
traceoptions]
[edit dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols oam gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping
traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery
traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[edit dynamic-profiles routing-instances instance routing-options multicast
traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance services mobile-ip
traceoptions]
[edit dynamic-profiles routing-instances instance system services
dhcp-local-server traceoptions]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options traceoptions]
[edit forwarding-options dhcp-relay interface-traceoptions]
[edit forwarding-options dhcp-relay traceoptions]
[edit jnx-example traceoptions]
```

```
[edit logical-systems vlans domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems vlans domain multicast-snooping-options traceoptions]
[edit logical-systems vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems forwarding-options dhcp-relay traceoptions]
[edit logical-systems protocols ancp traceoptions]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dot1x traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols ilmi traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols lacp traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam
traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam
traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options
dhcp-relay interface-traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options
dhcp-relay traceoptions]
[edit logical-systems routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor
```

```

traceoptions]
[edit logical-systems routing-instances instance protocols bgp group
traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp group
traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery
traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast
traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip
traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server interface-traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]

```

```
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay
traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance system services dhcp-local-server
interface-traceoptions]
[edit routing-instances instance system services dhcp-local-server traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
```

```

[edit services captive-portal-content-delivery]
[edit system ddos-protection traceoptions]
[edit services l2tp traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services server-load-balance traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services dhcp-local-server traceoptions]
[edit system services dhcp-local-server interface-traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)
- [trace on page 925](#)

view

Can view current system-wide, routing table, and protocol-specific values and statistics.

Commands

```

clear ipv6 router-advertisement
<clear-ipv6-router-advertisement-information>
<request-validation-policy>
show
show accounting

show accounting profile
<get-accounting-profile-information>

show accounting records
<get-accounting-record-information>

show amt
show amt statistics
<get-amt-statistics>

```

```
show amt summary
    <get-amt-summary>
show amt tunnel
    <get-amt-tunnel-information>
show amt tunnel gateway-address
    <get-amt-tunnel-gateway-address>
show amt tunnel tunnel-interface
    <get-amt-tunnel-interface>
show analytics collector
    <get-analytics-collector>
show ancp
show ancp cos
    <get-ancp-cos-information>
show ancp cos last-update
    <get-ancp-cos-last-update-information>

show ancp cos pending-update
    <get-ancp-cos-pending-information>

show ancp neighbor
    <get-ancp-neighbor-information>
show ancp statistics
    <get-ancp-stats-information>
show ancp subscriber
    <get-ancp-subscriber-information>

show ancp subscriber identifier
    <get-ancp-subscriber-identifier-information>
show ancp subscriber neighbor
show app-engine
show app-engine information
show app-engine packages
show app-engine packages remote
    <get-virtual-machine-package-remote>
show app-engine packages system
    <get-virtual-machine-package-system>
show app-engine processes
show app-engine resource-usage
show app-engine route-table
show app-engine routing-instance
show app-engine routing-instance compute-clusters
show app-engine routing-instance virtual-machines
show app-engine status
show app-engine virtual-machine package
    <get-virtual-machine-package-information>
show app-engine virtual-machine vm-instance
show aps
    <get-aps-information>

show aps group
    <get-aps-group-information>
show aps interface
    <get-aps-interface-information>
show arp
    <get-arp-table-information>

show as-path
    <get-as-path>
show as-path domain
    <get-as-path-domain>
show auto-configuration
```



```
show auto-configuration interfaces
show backup-selection
<get-backup-selection>
show backup-selection instance
<get-backup-selection-instance>
show bfd
show bfd session
  <get-bfd-session-information>

show bfd session address
  <get-bfd-session-address>
show bfd session client
  <get-bfd-session-client>
show bfd session client rsvp-oam
  <get-bfd-session-client-rsvp>
show bfd session client vpls-oam
  <get-bfd-session-client-vpls>
show bfd session client vpls-oam instance
  <get-bfd-session-client-vpls-instance>
show bfd session discriminator
  <get-bfd-session-discriminator>
show bfd session prefix
  <get-bfd-session-prefix>
show bfd subscriber
show bfd subscriber session
  <get-bfd-subscriber-session>
show bgp
show bgp bmp
  <get-bgp-monitoring-protocol-statistics>
show bgp group
  <get-bgp-group-information>

show bgp group rtf
  <get-bgp-rtf-information>

show bgp group traffic-statistics
  <get-bgp-traffic-statistics-information>

show bgp neighbor
  <get-bgp-neighbor-information>

show bgp neighbor orf
  <get-bgp-orf-information>

show bgp replication
  <get-bgp-replication-information>
show bgp summary
  <get-bgp-summary-information>

show bridge
show bridge domain
  <get-bridge-instance-information>

show bridge domain operational
  <get-operational-bridge-instance-information>
show bridge evpn
show bridge evpn arp-table
  <get-bridge-evpn-arp-table>
show bridge evpn peer-gateway-macs
  <get-bridge-peer-gateway-mac>
  <get-bridge-flood-information>
```

```
show bridge flood
show bridge flood event-queue
    <get-bridge-domain-event-queue-information>

show bridge flood route
show bridge flood route all-ce-flood
    <get-show-bridge-domain-all-ce-flood-route-information>

show bridge flood route all-ve-flood
    <get-show-bridge-domain-ve-flood-route-information>
show bridge flood route alt-root-flood
    <get-bridge-domain-alt-root-flood-route-information>
show bridge flood route bd-flood
    <get-bridge-domain-bd-flood-route-information>
show bridge flood route mlp-flood
    <get-bridge-domain-mlp-flood-route-information>
show bridge flood route re-flood
    <get-bridge-domain-re-flood-route-information>
show bridge mac-table
    <get-bridge-mac-table>
show bridge mac-table interface
    <get-bridge-interface-mac-table>
show bridge statistics
    <get-bridge-statistics-information>
show chassis
show chassis adc
show chassis alarms
    <get-alarm-information>
show chassis alarms fpc
    <get-fpc-alarm-information>
show chassis beacon
    <get-chassis-beacon-information>
show chassis beacon cb
    <get-chassis-cb-beacon-information>
show chassis environment adc
show chassis environment ccg
    <get-environment-ccg-information>
show chassis cfeb
    <get-cfeb-information>
show chassis cip
show chassis craft-interface
    <get-craft-information>
show chassis environment
    <get-environment-information>
show chassis environment cb
    <get-environment-cb-information>
show chassis environment cip
    <get-environment-cip-information>
show chassis environment feb
    <get-environment-feb-information>
show chassis environment fan
show chassis environment fpc
    <get-environment-fpc-information>
show chassis environment fpm
    <get-environment-fpm-information>
show chassis environment mcs
    <get-environment-mcs-information>
show chassis environment pcg
    <get-environment-pcg-information>
show chassis environment pdu
    <get-environment-pdu-information>
```

```
show chassis environment pem
  <get-environment-pem-information>
show chassis environment psm
show chassis environment psu
  <get-environment-psu-information>
show chassis environment routing-engine
  <get-environment-re-information>
show chassis environment scg
  <get-environment-scg-information>
show chassis environment service-node
  <get-environment-service-node-information>
show chassis environment sfb
show chassis environment sfm
  <get-environment-sfm-information>

show chassis environment sib
  <get-environment-sib-information>

show chassis environment sib f13
show chassis environment sib f2s
show chassis ethernet-switch
show chassis ethernet-switch errors
show chassis ethernet-switch statistics
show chassis ethernet-switch temperature
show chassis fabric
show chassis fabric degraded-fabric-reachability
show chassis fabric device
  <get-chassis-fabric-information-device>
show chassis fabric connectivity
  <get-chassis-fabric-connectivity-information>
show chassis fabric degradation
  <get-fm-degradation-information>
show chassis fabric degradation actions
  <get-fm-degradation-information-details>
show chassis fabric destinations
  <get-fm-fabric-destinations-state>
show chassis fabric errors
show chassis fabric errors autoheal
  <get-fm-plane-autoheal-errors>
show chassis fabric errors fpc
  <get-fm-fpc-errors>

show chassis fabric errors sib
  <get-fm-sib-errors>

show chassis fabric errors sib f13
show chassis fabric errors sib f2s
show chassis fabric feb
show chassis fabric fpcs
  <get-fm-fpc-state-information>

show chassis fabric links
  <get-chassis-fabric-link-information>
show chassis fabric map
show chassis fabric plane
  <get-fm-plane-state-information>

show chassis fabric plane-location
show chassis fabric reachability
  <get-fm-fabric-reachability-information>
show chassis fabric sibs
```

```
<get-fm-sib-state-information>
show chassis fabric spray-weights
  <get-chassis-fabric-spray-weight-information>
show chassis fabric spray-weights from
show chassis fabric spray-weights to
show chassis fabric summary
  <get-fm-state-information>

show chassis fabric topology
  <get-chassis-fabric-topology-information>
show chassis fabric unreachable-destinations
  <get-fm-unreachable-dest-information>
show chassis fan
show chassis feb
  <get-feb-brief-information>

show chassis feb detail
  <get-feb-information>

show chassis firmware
  <get-firmware-information>

show chassis firmware detail
  <get-firmware-information-detail>
show chassis forwarding
  <get-fwdd-information>

show chassis fpc
  <get-fpc-information>

show chassis fpc errors
  <get-fpc-error-information>

show chassis fpc pic-status
  <get-pic-information>

show chassis fpc-feb-connectivity
  <get-fpc-feb-connectivity-information>

show chassis hardware
  <get-chassis-inventory>
show chassis hss
show chassis hss link-quality
show chassis in-service-upgrade
show chassis ioc-npc-connectivity
  <get-ioc-npc-connectivity-information>

show chassis lccs
  <get-fru-information>

show chassis location
  <get-chassis-location>

show chassis location fpc
show chassis location interface
show chassis location interface by-name
  <get-interface-location-name-information>

show chassis location interface by-slot
  <get-interface-location-information>
show chassis mac-addresses
```

```
show chassis multicast-loadbalance
<get-chassis-ae-lb-information>

show chassis network-services
<network-services>

show chassis nonstop-upgrade
show chassis pic
<get-pic-detail>

show chassis power
<get-power-usage-information>

show chassis power detail
<get-power-usage-information-detail>
show chassis power sequence
show chassis power upgrade

show chassis power-ratings
<get-power-management>

show chassis psd
<get-psd-information>

show chassis redundancy
show chassis redundancy feb
<get-feb-redundancy-information>

show chassis redundancy feb errors
<get-feb-redundancy-error-information>

show chassis redundancy feb redundancy-group
<get-feb-redundancy-group-information>

show chassis redundant-power-system
<get-rps-chassis-information>

show chassis routing-engine
<get-route-engine-information>

show chassis routing-engine bios
<get-bios-version-information>
show chassis scb
<get-scb-information>

show chassis service-node
<get-service-node-information>

show chassis sfm
<get-sfm-information>

show chassis sfm detail
show chassis sibs
<get-sib-information>

show chassis spmb
<get-spmb-information>

show chassis spmb sibs
<get-spmb-sib-information>
```

```
show chassis ssb
    <get-ssb-information>

show chassis synchronization
    <get-clock-synchronization-information>

show chassis synchronization backup
show chassis synchronization master
show chassis system-mode
<get-system-mode-information>
show chassis temperature-thresholds
    <get-temperature-threshold-information>
show chassis vcpu
show chassis zones
    <get-chassis-zones-information>
show class-of-service
    <get-cos-information>

show class-of-service adaptive-shaper
    <get-cos-adaptive-shaper-information>

show class-of-service application-traffic-control
show class-of-service application-traffic-control counter
show class-of-service application-traffic-control statistics
show class-of-service application-traffic-control statistics rate-limiter
show class-of-service application-traffic-control statistics rule
    <get-appqos-rule-statistics>
show class-of-service classifier
    <get-cos-classifier-information>

show class-of-service code-point-aliases
    <get-cos-code-point-map-information>

show class-of-service congestion-notification
    <get-cos-congestion-notification-information>
show class-of-service drop-profile
    <get-cos-drop-profile-information>

show class-of-service fabric
show class-of-service fabric scheduler-map
    <get-cos-fabric-scheduler-map-information>

show class-of-service fabric statistics
    <get-fabric-queue-information>

show class-of-service fabric statistics detail
    <get-fabric-queue-detailed-information>

show class-of-service forwarding-class
    <get-cos-forwarding-class-information>

show class-of-service forwarding-class-set
    <get-cos-forwarding-class-set-information>
show class-of-service forwarding-table
    <get-cos-table-information>

show class-of-service forwarding-table classifier
    <get-cos-classifier-table-information>

show class-of-service forwarding-table classifier mapping
    <get-cos-classifier-table-map-information>
```

```
show class-of-service forwarding-table drop-profile
  <get-cos-red-information>

show class-of-service forwarding-table fabric
show class-of-service forwarding-table fabric scheduler-map
  <get-cos-fwtab-fabric-scheduler-map-information>

show class-of-service forwarding-table forwarding-class-map
  <get-cos-forwarding-class-map-table-information>

show class-of-service forwarding-table forwarding-class-map mapping
  <get-cos-forwarding-class-map-interface-table-information>

show class-of-service forwarding-table loss-priority-map
  <get-cos-loss-priority-map-table-information>

show class-of-service forwarding-table loss-priority-map mapping
  <get-cos-loss-priority-map-table-binding-information>

show class-of-service forwarding-table loss-priority-rewrite
  <get-cos-loss-priority-rewrite-table-information>
show class-of-service forwarding-table loss-priority-rewrite mapping
  <get-cos-loss-priority-rewrite-table-binding-information>
show class-of-service forwarding-table policer
  <get-cos-policer-table-map-information>

show class-of-service forwarding-table rewrite-rule
  <get-cos-rewrite-table-information>

show class-of-service forwarding-table rewrite-rule mapping
  <get-cos-rewrite-table-map-information>

show class-of-service forwarding-table scheduler-map
  <get-cos-scheduler-map-table-information>

show class-of-service forwarding-table shaper
  <get-cos-shaper-table-map-information>

show class-of-service forwarding-table translation-table
  <get-cos-translation-table-information>

show class-of-service forwarding-table translation-table mapping
  <get-cos-translation-table-mapping-information>

show class-of-service fragmentation-map
  <get-cos-fragmentation-map-information>

show class-of-service interface
  <get-cos-interface-map-information>

show class-of-service interface-set
  <get-cos-interface-set-map-information>

show class-of-service l2tp-session
  <get-cos-l2tp-session-map-information>

show class-of-service loss-priority-map
  <get-cos-loss-priority-map-information>

show class-of-service loss-priority-rewrite
```

```
<get-cos-loss-priority-rewrite-information>
show class-of-service multi-destination
  <get-cos-multi-destination-information>

show class-of-service packet-buffer
  <get-cos-packet-buffer-information>
show class-of-service packet-buffer usage
  <get-cos-packet-buffer-usage-information>

show class-of-service rewrite-rule
  <get-cos-rewrite-information>

show class-of-service routing-instance
  <get-cos-routing-instance-map-information>

show class-of-service scheduler-hierarchy
show class-of-service scheduler-hierarchy interface
  <get-interface-scheduler-hierarchy-information>

show class-of-service scheduler-hierarchy interface-set
  <get-interface-set-scheduler-hierarchy-information>

show class-of-service scheduler-map
  <get-cos-scheduler-map-information>

show class-of-service traffic-control-profile
  <get-cos-traffic-control-profile-information>

show class-of-service translation-table
  <get-cos-translation-table-map-information>

show class-of-service virtual-channel
  <get-cos-virtual-channel-information>

show class-of-service virtual-channel-group
  <get-cos-virtual-channel-group-information>

show cli
show cli authorization
  <get-authorization-information>

show cli directory
  <get-current-working-directory>
show cli history
show configuration
show connections
  <get-ccc-information>
show database-replication
show database-replication statistics
  <get-database-replication-statistics-information>

show database-replication summary
  <get-database-replication-summary-information>
show ddos-protection
show ddos-protection protocols
  <get-ddos-protocols-information>
show ddos-protection protocols amtv4
show ddos-protection protocols amtv4 aggregate
show ddos-protection protocols amtv4 aggregate culprit-flows
show ddos-protection protocols amtv4 culprit-flows
show ddos-protection protocols amtv4 flow-detection
```



```
show ddos-protection protocols amtv4 parameters
show ddos-protection protocols amtv4 statistics
show ddos-protection protocols amtv4 violations
show ddos-protection protocols amtv6
show ddos-protection protocols amtv6 aggregate
show ddos-protection protocols amtv6 aggregate culprit-flows
show ddos-protection protocols amtv6 culprit-flows
show ddos-protection protocols amtv6 flow-detection
show ddos-protection protocols amtv6 statistics
show ddos-protection protocols amtv6 violations
```

```
show ddos-protection protocols ancp
  <get-ddos-ancp-information>

show ddos-protection protocols ancp aggregate
  <get-ddos-ancp-aggregate>
show ddos-protection protocols ancp parameters
  <get-ddos-ancp-parameters>

show ddos-protection protocols ancp statistics
  <get-ddos-ancp-statistics>
show ddos-protection protocols ancp violations
  <get-ddos-ancp-violations>
show ddos-protection protocols ancpv6
  <get-ddos-ancpv6-information>
show ddos-protection protocols ancpv6 aggregate
  get-ddos-ancpv6-aggregate
show ddos-protection protocols ancpv6 parameters
  get-ddos-ancpv6-parameters
show ddos-protection protocols ancpv6 statistics
  get-ddos-ancpv6-statistics
show ddos-protection protocols ancpv6 violations
  get-ddos-ancpv6-violations
show ddos-protection protocols arp
  get-ddos-arp-information
show ddos-protection protocols arp aggregate
  get-ddos-arp-aggregate
show ddos-protection protocols arp parameters
  get-ddos-arp-parameters
show ddos-protection protocols arp statistics
  get-ddos-arp-statistics
show ddos-protection protocols arp violations
  get-ddos-arp-violations
show ddos-protection protocols atm
  get-ddos-atm-information
show ddos-protection protocols atm aggregate
  get-ddos-atm-aggregate
show ddos-protection protocols atm parameters
  get-ddos-atm-parameters
show ddos-protection protocols atm statistics
  get-ddos-atm-statistics
show ddos-protection protocols atm violations
  get-ddos-atm-violations
show ddos-protection protocols bfd
  get-ddos-bfd-information
show ddos-protection protocols bfd aggregate
  get-ddos-bfd-aggregate
show ddos-protection protocols bfd parameters
  get-ddos-bfd-parameters
show ddos-protection protocols bfd statistics
```

```
get-ddos-bfd-statistics
show ddos-protection protocols bfd violations
get-ddos-bfd-violations
show ddos-protection protocols bfdv6
get-ddos-bfdv6-information
show ddos-protection protocols bfdv6 aggregate
get-ddos-bfdv6-aggregate
show ddos-protection protocols bfdv6 parameters
get-ddos-bfdv6-parameters
show ddos-protection protocols bfdv6 statistics
get-ddos-bfdv6-statistics
show ddos-protection protocols bfdv6 violations
get-ddos-bfdv6-violations
show ddos-protection protocols bgp
get-ddos-bgp-information
show ddos-protection protocols bgp aggregate
get-ddos-bgp-aggregate
show ddos-protection protocols bgp parameters
get-ddos-bgp-parameters
show ddos-protection protocols bgp statistics
get-ddos-bgp-statistics
show ddos-protection protocols bgp violations
get-ddos-bgp-violations
show ddos-protection protocols bgpv6
get-ddos-bgpv6-information
show ddos-protection protocols bgpv6 aggregate
get-ddos-bgpv6-aggregate
show ddos-protection protocols bgpv6 parameters
get-ddos-bgpv6-parameters
show ddos-protection protocols bgpv6 statistics
get-ddos-bgpv6-statistics
show ddos-protection protocols bgpv6 violations
get-ddos-bgpv6-violations
show ddos-protection protocols demux-autosense
get-ddos-demuxauto-information
show ddos-protection protocols demux-autosense aggregate
get-ddos-demuxauto-aggregate
show ddos-protection protocols demux-autosense parameters
get-ddos-demuxauto-parameters
show ddos-protection protocols demux-autosense statistics
get-ddos-demuxauto-statistics
show ddos-protection protocols demux-autosense violations
get-ddos-demuxauto-violations
show ddos-protection protocols dhcpv4
get-ddos-dhcpv4-information
show ddos-protection protocols dhcpv4 ack
get-ddos-dhcpv4-ack
show ddos-protection protocols dhcpv4 aggregate
get-ddos-dhcpv4-aggregate
show ddos-protection protocols dhcpv4 bad-packets
get-ddos-dhcpv4-bad-pack
show ddos-protection protocols dhcpv4 bootp
get-ddos-dhcpv4-bootp
show ddos-protection protocols dhcpv4 decline
get-ddos-dhcpv4-decline
show ddos-protection protocols dhcpv4 discover
get-ddos-dhcpv4-discover
show ddos-protection protocols dhcpv4 force-renew
get-ddos-dhcpv4-forcerenew
show ddos-protection protocols dhcpv4 inform
get-ddos-dhcpv4-inform
```

```
show ddos-protection protocols dhcpv4 lease-active
  get-ddos-dhcpv4-leaseact
show ddos-protection protocols dhcpv4 lease-query
  get-ddos-dhcpv4-leasequery
show ddos-protection protocols dhcpv4 lease-unassigned
  get-ddos-dhcpv4-leaseuna
show ddos-protection protocols dhcpv4 lease-unknown
  get-ddos-dhcpv4-leaseunk
show ddos-protection protocols dhcpv4 nak
  get-ddos-dhcpv4-nak
show ddos-protection protocols dhcpv4 no-message-type
  get-ddos-dhcpv4-no-msgtype
show ddos-protection protocols dhcpv4 offer
  get-ddos-dhcpv4-offer
show ddos-protection protocols dhcpv4 offer culprit-flows
show ddos-protection protocols dhcpv4 parameters
  get-ddos-dhcpv4-parameters
show ddos-protection protocols dhcpv4 release
  get-ddos-dhcpv4-release
show ddos-protection protocols dhcpv4 renew
  get-ddos-dhcpv4-renew
show ddos-protection protocols dhcpv4 request
  get-ddos-dhcpv4-request
show ddos-protection protocols dhcpv4 statistics
  get-ddos-dhcpv4-statistics
show ddos-protection protocols dhcpv4 unclassified
  get-ddos-dhcpv4-unclass
show ddos-protection protocols dhcpv4 violations
  get-ddos-dhcpv4-violations
show ddos-protection protocols dhcpv4v6
  <get-ddos-dhcpv4v6-information>
show ddos-protection protocols dhcpv4v6 aggregate
  <get-ddos-dhcpv4v6-aggregate>
show ddos-protection protocols dhcpv4v6 aggregate culprit-flows
  <get-ddos-dhcpv4v6-aggregate-flows>
show ddos-protection protocols dhcpv4v6 culprit-flows
  <get-ddos-dhcpv4v6-flows>
show ddos-protection protocols dhcpv4v6 flow-detection
  <get-ddos-dhcpv4v6-flow-parameters>
show ddos-protection protocols dhcpv4v6 parameters
  <get-ddos-dhcpv4v6-parameters>
show ddos-protection protocols dhcpv4v6 statistics
  <get-ddos-dhcpv4v6-statistics>
show ddos-protection protocols dhcpv4v6 violations
  <get-ddos-dhcpv4v6-violations>
show ddos-protection protocols dhcpv6
  get-ddos-dhcpv6-information
show ddos-protection protocols dhcpv6 advertise
  get-ddos-dhcpv6-advertise
show ddos-protection protocols dhcpv6 advertise culprit-flows
show ddos-protection protocols dhcpv6 aggregate
  get-ddos-dhcpv6-aggregate
show ddos-protection protocols dhcpv6 confirm
  get-ddos-dhcpv6-confirm
show ddos-protection protocols dhcpv6 decline
  get-ddos-dhcpv6-decline
show ddos-protection protocols dhcpv6 information-request
  get-ddos-dhcpv6-info-req
show ddos-protection protocols dhcpv6 leasequery
  get-ddos-dhcpv6-leasequery
show ddos-protection protocols dhcpv6 leasequery culprit-flows
```

```
show ddos-protection protocols dhcpv6 leasequery-data
  get-ddos-dhcpv6-leaseq-da
show ddos-protection protocols dhcpv6 leasequery-done
  get-ddos-dhcpv6-leaseq-do
show ddos-protection protocols dhcpv6 leasequery-reply
  get-ddos-dhcpv6-leaseq-re
show ddos-protection protocols dhcpv6 parameters
  get-ddos-dhcpv6-parameters
show ddos-protection protocols dhcpv6 rebind
  get-ddos-dhcpv6-rebind
show ddos-protection protocols dhcpv6 reconfigure
  get-ddos-dhcpv6-reconfig
show ddos-protection protocols dhcpv6 relay-forward
  get-ddos-dhcpv6-relay-for
show ddos-protection protocols dhcpv6 relay-reply
  get-ddos-dhcpv6-relay-rep
show ddos-protection protocols dhcpv6 release
  get-ddos-dhcpv6-release
show ddos-protection protocols dhcpv6 renew
  get-ddos-dhcpv6-renew
show ddos-protection protocols dhcpv6 reply
  get-ddos-dhcpv6-reply
show ddos-protection protocols dhcpv6 request
  get-ddos-dhcpv6-request
show ddos-protection protocols dhcpv6 solicit
  get-ddos-dhcpv6-solicit
show ddos-protection protocols dhcpv6 statistics
  get-ddos-dhcpv6-statistics
show ddos-protection protocols dhcpv6 unclassified
  get-ddos-dhcpv6-unclass
show ddos-protection protocols dhcpv6 unclassified culprit-flows
show ddos-protection protocols dhcpv6 violations
  get-ddos-dhcpv6-violations
show ddos-protection protocols diameter
  get-ddos-diameter-information
show ddos-protection protocols diameter aggregate
  get-ddos-diameter-aggregate
show ddos-protection protocols diameter parameters
  get-ddos-diameter-parameters
show ddos-protection protocols diameter statistics
  get-ddos-diameter-statistics
show ddos-protection protocols diameter violations
  get-ddos-diameter-violations
show ddos-protection protocols dns
  get-ddos-dns-information
show ddos-protection protocols dns aggregate
  get-ddos-dns-aggregate
show ddos-protection protocols dns parameters
  get-ddos-dns-parameters
show ddos-protection protocols dns statistics
  get-ddos-dns-statistics
show ddos-protection protocols dns violations
  get-ddos-dns-violations
show ddos-protection protocols dtcp
  get-ddos-dtcp-information
show ddos-protection protocols dtcp aggregate
  get-ddos-dtcp-aggregate
show ddos-protection protocols dtcp aggregate culprit-flows
show ddos-protection protocols dtcp parameters
  get-ddos-dtcp-parameters
show ddos-protection protocols dtcp statistics
```

```
get-ddos-dtcp-statistics
show ddos-protection protocols dtcp violations
get-ddos-dtcp-violations
show ddos-protection protocols dynamic-vlan
get-ddos-dynvlan-information
show ddos-protection protocols dynamic-vlan aggregate
get-ddos-dynvlan-aggregate
show ddos-protection protocols dynamic-vlan parameters
get-ddos-dynvlan-parameters
show ddos-protection protocols dynamic-vlan statistics
get-ddos-dynvlan-statistics
show ddos-protection protocols dynamic-vlan violations
get-ddos-dynvlan-violations
show ddos-protection protocols egpv6
get-ddos-egpv6-information
show ddos-protection protocols egpv6 aggregate
get-ddos-egpv6-aggregate
show ddos-protection protocols egpv6 parameters
get-ddos-egpv6-parameters
show ddos-protection protocols egpv6 statistics
get-ddos-egpv6-statistics
show ddos-protection protocols egpv6 violations
get-ddos-egpv6-violations
show ddos-protection protocols eoam
get-ddos-eoam-information
show ddos-protection protocols eoam aggregate
get-ddos-eoam-aggregate
show ddos-protection protocols eoam parameters
get-ddos-eoam-parameters
show ddos-protection protocols eoam statistics
get-ddos-eoam-statistics
show ddos-protection protocols eoam violations
get-ddos-eoam-violations
show ddos-protection protocols esmc
get-ddos-esmc-information
show ddos-protection protocols esmc aggregate
get-ddos-esmc-aggregate
show ddos-protection protocols esmc parameters
get-ddos-esmc-parameters
show ddos-protection protocols esmc statistics
get-ddos-esmc-statistics
show ddos-protection protocols esmc violations
get-ddos-esmc-violations
show ddos-protection protocols fab-probe
<get-ddos-fab-probe-information>
show ddos-protection protocols fab-probe aggregate
<get-ddos-fab-probe-aggregate>
show ddos-protection protocols fab-probe parameters
<get-ddos-fab-probe-parameters>
show ddos-protection protocols fab-probe statistics
<get-ddos-fab-probe-statistics>
show ddos-protection protocols fab-probe violations
<get-ddos-fab-probe-violations>
show ddos-protection protocols firewall-host
get-ddos-fw-host-information
show ddos-protection protocols firewall-host aggregate
get-ddos-fw-host-aggregate
show ddos-protection protocols firewall-host parameters
get-ddos-fw-host-parameters
show ddos-protection protocols firewall-host statistics
get-ddos-fw-host-statistics
```

```
show ddos-protection protocols firewall-host violations
get-ddos-fw-host-violations
```

```
show ddos-protection protocols ftp
  get-ddos-ftp-information
show ddos-protection protocols ftp aggregate
  get-ddos-ftp-aggregate
show ddos-protection protocols ftp parameters
  get-ddos-ftp-parameters
show ddos-protection protocols ftp statistics
  get-ddos-ftp-statistics
show ddos-protection protocols ftp violations
  get-ddos-ftp-violations
show ddos-protection protocols ftpv6
  get-ddos-ftpv6-information
show ddos-protection protocols ftpv6 aggregate
  get-ddos-ftpv6-aggregate
show ddos-protection protocols ftpv6 parameters
  get-ddos-ftpv6-parameters
show ddos-protection protocols ftpv6 statistics
  get-ddos-ftpv6-statistics
show ddos-protection protocols ftpv6 violations
  get-ddos-ftpv6-violations
show ddos-protection protocols garp-reply
  <get-ddos-garp-reply-information>
show ddos-protection protocols garp-reply aggregate
  <get-ddos-garp-reply-aggregate>
show ddos-protection protocols garp-reply aggregate culprit-flows
  <get-ddos-garp-reply-aggregate-flows>
show ddos-protection protocols garp-reply culprit-flows
  <get-ddos-garp-reply-flows>
show ddos-protection protocols garp-reply flow-detection
  <get-ddos-garp-reply-flow-parameters>
show ddos-protection protocols garp-reply parameters
  <get-ddos-garp-reply-parameters>
show ddos-protection protocols garp-reply statistics
  <get-ddos-garp-reply-statistics>
show ddos-protection protocols garp-reply violations
  <get-ddos-garp-reply-violations>
show ddos-protection protocols gre
  get-ddos-gre-information
show ddos-protection protocols gre aggregate
  get-ddos-gre-aggregate
show ddos-protection protocols gre hbc
  <get-ddos-gre-hbc>
show ddos-protection protocols gre hbc culprit-flows
  <get-ddos-gre-hbc-flows>
show ddos-protection protocols gre parameters
  get-ddos-gre-parameters
show ddos-protection protocols gre punt
  <get-ddos-gre-punt>
show ddos-protection protocols gre punt culprit-flows
  <get-ddos-gre-punt-flows>
show ddos-protection protocols gre statistics
  get-ddos-gre-statistics
show ddos-protection protocols gre violations
  get-ddos-gre-violations
show ddos-protection protocols icmp
  get-ddos-icmp-information
show ddos-protection protocols icmp aggregate
```

```
get-ddos-icmp-aggregate
show ddos-protection protocols icmp parameters
get-ddos-icmp-parameters
show ddos-protection protocols icmp statistics
get-ddos-icmp-statistics
show ddos-protection protocols icmp violations
get-ddos-icmp-violations
show ddos-protection protocols icmpv6
<get-ddos-icmpv6-information>
show ddos-protection protocols icmpv6 aggregate
<get-ddos-icmpv6-aggregate>
show ddos-protection protocols icmpv6 aggregate culprit-flows
<get-ddos-icmpv6-aggregate-flows>
show ddos-protection protocols icmpv6 parameters
<get-ddos-icmpv6-parameters>
show ddos-protection protocols icmpv6 statistics
<get-ddos-icmpv6-statistics>
show ddos-protection protocols icmpv6 violations
<get-ddos-icmpv6-violations>
show ddos-protection protocols igmp
get-ddos-igmp-information
show ddos-protection protocols igmp aggregate
get-ddos-igmp-aggregate
show ddos-protection protocols igmp aggregate culprit-flows
show ddos-protection protocols igmp parameters
get-ddos-igmp-parameters
show ddos-protection protocols igmp statistics
get-ddos-igmp-statistics
show ddos-protection protocols igmp violations
get-ddos-igmp-violations
show ddos-protection protocols igmp-snoop
get-ddos-igmp-snoop-information
show ddos-protection protocols igmp-snoop aggregate
get-ddos-igmp-snoop-aggregate
show ddos-protection protocols igmp-snoop parameters
get-ddos-igmp-snoop-parameters
show ddos-protection protocols igmp-snoop statistics
get-ddos-igmp-snoop-statistics
show ddos-protection protocols igmp-snoop violations
get-ddos-igmp-snoop-violations
show ddos-protection protocols igmpv4v6
get-ddos-igmpv4v6-information
show ddos-protection protocols igmpv4v6 aggregate
get-ddos-igmpv4v6-aggregate
show ddos-protection protocols igmpv4v6 aggregate culprit-flows
show ddos-protection protocols igmpv4v6 parameters
get-ddos-igmpv4v6-parameters
show ddos-protection protocols igmpv4v6 statistics
get-ddos-igmpv4v6-statistics
show ddos-protection protocols igmpv4v6 violations
get-ddos-igmpv4v6-violations
show ddos-protection protocols igmpv6
get-ddos-igmpv6-information
show ddos-protection protocols igmpv6 aggregate
get-ddos-igmpv6-aggregate
show ddos-protection protocols igmpv6 parameters
get-ddos-igmpv6-parameters
show ddos-protection protocols igmpv6 statistics
get-ddos-igmpv6-statistics
show ddos-protection protocols igmpv6 violations
get-ddos-igmpv6-violations
```

```
show ddos-protection protocols ip-fragments
  get-ddos-ip-frag-information
show ddos-protection protocols ip-fragments aggregate
  get-ddos-ip-frag-aggregate
show ddos-protection protocols ip-fragments first-fragment
  get-ddos-ip-frag-first-frag
show ddos-protection protocols ip-fragments parameters
  get-ddos-ip-frag-parameters
show ddos-protection protocols ip-fragments statistics
  get-ddos-ip-frag-statistics
show ddos-protection protocols ip-fragments trail-fragment
  get-ddos-ip-frag-trail-frag
show ddos-protection protocols ip-fragments violations
  get-ddos-ip-frag-violations
show ddos-protection protocols ip-options
  get-ddos-ip-opt-information
show ddos-protection protocols ip-options aggregate
  get-ddos-ip-opt-aggregate
show ddos-protection protocols ip-options non-v4v6
<get-ddos-ip-opt-non-v4v6>
show ddos-protection protocols ip-options parameters
  get-ddos-ip-opt-parameters
show ddos-protection protocols ip-options router-alert
  get-ddos-ip-opt-rt-alert
show ddos-protection protocols ip-options statistics
  get-ddos-ip-opt-statistics
show ddos-protection protocols ip-options unclassified
  get-ddos-ip-opt-unclass
show ddos-protection protocols ipmc-reserved culprit-flows
<get-ddos-ipmc-reserved-flows>
show ddos-protection protocols ipmc-reserved flow-detection
<get-ddos-ipmc-reserved-flow-parameters>
show ddos-protection protocols ipmc-reserved parameters
<get-ddos-ipmc-reserved-parameters>
show ddos-protection protocols ipmc-reserved statistics
<get-ddos-ipmc-reserved-statistics>
show ddos-protection protocols ipmc-reserved violations
<get-ddos-ipmc-reserved-violations>
show ddos-protection protocols ipmcast-miss
<get-ddos-ipmcast-miss-information>
show ddos-protection protocols ipmcast-miss aggregate
<get-ddos-ipmcast-miss-aggregate>
show ddos-protection protocols ipmcast-miss aggregate culprit-flows
<get-ddos-ipmcast-miss-aggregate-flows>
show ddos-protection protocols ipmcast-miss culprit-flows
<get-ddos-ipmcast-miss-flows>
show ddos-protection protocols ipmcast-miss flow-detection
<get-ddos-ipmcast-miss-flow-parameters>
show ddos-protection protocols ipmcast-miss parameters
<get-ddos-ipmcast-miss-parameters>
show ddos-protection protocols ipmcast-miss statistics
<get-ddos-ipmcast-miss-statistics>
show ddos-protection protocols ipmcast-miss violations
<get-ddos-ipmcast-miss-violations>
show ddos-protection protocols ip-options violations
  get-ddos-ip-opt-violations
show ddos-protection protocols ipv4-unclassified
  get-ddos-ipv4-uncls-information
show ddos-protection protocols ipv4-unclassified aggregate
  get-ddos-ipv4-uncls-aggregate
show ddos-protection protocols ipv4-unclassified parameters
```



```

get-ddos-ipv4-uncls-parameters
show ddos-protection protocols ipv4-unclassified statistics
get-ddos-ipv4-uncls-statistics
show ddos-protection protocols ipv4-unclassified violations
get-ddos-ipv4-uncls-violations
show ddos-protection protocols ipv6-unclassified
get-ddos-ipv6-uncls-information
show ddos-protection protocols ipv6-unclassified aggregate
get-ddos-ipv6-uncls-aggregate
show ddos-protection protocols ipv6-unclassified parameters
get-ddos-ipv6-uncls-parameters
show ddos-protection protocols ipv6-unclassified statistics
get-ddos-ipv6-uncls-statistics
show ddos-protection protocols ipv6-unclassified violations
get-ddos-ipv6-uncls-violations
show ddos-protection protocols isis
get-ddos-isis-information
show ddos-protection protocols isis aggregate
get-ddos-isis-aggregate
show ddos-protection protocols isis parameters
get-ddos-isis-parameters
show ddos-protection protocols isis statistics
get-ddos-isis-statistics
show ddos-protection protocols isis violations
get-ddos-isis-violations
show ddos-protection protocols jfm
get-ddos-jfm-information
show ddos-protection protocols jfm aggregate
get-ddos-jfm-aggregate
show ddos-protection protocols jfm parameters
get-ddos-jfm-parameters
show ddos-protection protocols jfm statistics
get-ddos-jfm-statistics
show ddos-protection protocols jfm violations
get-ddos-jfm-violations
show ddos-protection protocols l2tp
get-ddos-l2tp-information
show ddos-protection protocols l2tp aggregate
get-ddos-l2tp-aggregate
show ddos-protection protocols l2tp parameters
get-ddos-l2tp-parameters
show ddos-protection protocols l2tp statistics
get-ddos-l2tp-statistics
show ddos-protection protocols l2tp violations
get-ddos-l2tp-violations
show ddos-protection protocols l3dest-miss
  <get-ddos-l3dest-miss-information>
show ddos-protection protocols l3dest-miss aggregate
  <get-ddos-l3dest-miss-aggregate>
show ddos-protection protocols l3dest-miss aggregate culprit-flows
  <get-ddos-l3dest-miss-aggregate-flows>
show ddos-protection protocols l3dest-miss culprit-flows
  <get-ddos-l3dest-miss-flows>
show ddos-protection protocols l3dest-miss flow-detection
  <get-ddos-l3dest-miss-flow-parameters>
show ddos-protection protocols l3dest-miss parameters
  <get-ddos-l3dest-miss-parameters>
show ddos-protection protocols l3dest-miss statistics
  <get-ddos-l3dest-miss-statistics>
show ddos-protection protocols l3dest-miss violations
  <get-ddos-l3dest-miss-violations>

```

```
show ddos-protection protocols l3mc-sgv-hit-icl
  <get-ddos-l3mc-sgv-hit-icl-information>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate
  <get-ddos-l3mc-sgv-hit-icl-aggregate>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
  <get-ddos-l3mc-sgv-hit-icl-aggregate-flows>
show ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
  <get-ddos-l3mc-sgv-hit-icl-flows>
show ddos-protection protocols l3mc-sgv-hit-icl flow-detection
  <get-ddos-l3mc-sgv-hit-icl-flow-parameters>
show ddos-protection protocols l3mc-sgv-hit-icl parameters
  <get-ddos-l3mc-sgv-hit-icl-parameters>
show ddos-protection protocols l3mc-sgv-hit-icl statistics
  <get-ddos-l3mc-sgv-hit-icl-statistics>
show ddos-protection protocols l3mc-sgv-hit-icl violations
  <get-ddos-l3mc-sgv-hit-icl-violations>
show ddos-protection protocols l3mtu-fail
  <get-ddos-l3mtu-fail-information>
show ddos-protection protocols l3mtu-fail aggregate
  <get-ddos-l3mtu-fail-aggregate>
show ddos-protection protocols l3mtu-fail aggregate culprit-flows
  <get-ddos-l3mtu-fail-aggregate-flows>
show ddos-protection protocols l3mtu-fail culprit-flows
  <get-ddos-l3mtu-fail-flows>
show ddos-protection protocols l3mtu-fail flow-detection
  <get-ddos-l3mtu-fail-flow-parameters>
show ddos-protection protocols l3mtu-fail parameters
  <get-ddos-l3mtu-fail-parameters>
show ddos-protection protocols l3mtu-fail statistics
  <get-ddos-l3mtu-fail-statistics>
show ddos-protection protocols l3mtu-fail violations
  <get-ddos-l3mtu-fail-violations>
show ddos-protection protocols l3nhop
  <get-ddos-l3nhop-information>
show ddos-protection protocols l3nhop aggregate
  <get-ddos-l3nhop-aggregate>
show ddos-protection protocols l3nhop aggregate culprit-flows
  <get-ddos-l3nhop-aggregate-flows>
show ddos-protection protocols l3nhop culprit-flows
  <get-ddos-l3nhop-flows>
show ddos-protection protocols l3nhop flow-detection
  <get-ddos-l3nhop-flow-parameters>
show ddos-protection protocols l3nhop parameters
  <get-ddos-l3nhop-parameters>
show ddos-protection protocols l3nhop statistics
  <get-ddos-l3nhop-statistics>
show ddos-protection protocols l3nhop violations
  <get-ddos-l3nhop-violations>
show ddos-protection protocols lacp
  <get-ddos-lacp-information>
show ddos-protection protocols lacp aggregate
  <get-ddos-lacp-aggregate>
show ddos-protection protocols lacp parameters
  <get-ddos-lacp-parameters>
show ddos-protection protocols lacp statistics
  <get-ddos-lacp-statistics>
show ddos-protection protocols lacp violations
  <get-ddos-lacp-violations>
show ddos-protection protocols ldp
  <get-ddos-ldp-information>
show ddos-protection protocols ldp aggregate
```

```

<get-ddos-ldp-aggregate>
show ddos-protection protocols ldp parameters
<get-ddos-ldp-parameters>
show ddos-protection protocols ldp statistics
<get-ddos-ldp-statistics>
show ddos-protection protocols ldp violations
<get-ddos-ldp-violations>
show ddos-protection protocols ldpv6
<get-ddos-ldpv6-information>
show ddos-protection protocols ldpv6 aggregate
<get-ddos-ldpv6-aggregate>
show ddos-protection protocols ldpv6 parameters
<get-ddos-ldpv6-parameters>
show ddos-protection protocols ldpv6 statistics
<get-ddos-ldpv6-statistics>
show ddos-protection protocols ldpv6 violations
<get-ddos-ldpv6-violations>
show ddos-protection protocols lldp
<get-ddos-lldp-information>
show ddos-protection protocols lldp aggregate
<get-ddos-lldp-aggregate>
show ddos-protection protocols lldp parameters
<get-ddos-lldp-parameters>
show ddos-protection protocols lldp statistics
<get-ddos-lldp-statistics>
show ddos-protection protocols lldp violations
<get-ddos-lldp-violations>
show ddos-protection protocols lmp
<get-ddos-lmp-information>
show ddos-protection protocols lmp aggregate
<get-ddos-lmp-aggregate>
show ddos-protection protocols lmp parameters
<get-ddos-lmp-parameters>
show ddos-protection protocols lmp statistics
<get-ddos-lmp-statistics>
show ddos-protection protocols lmp violations
<get-ddos-lmp-violations>
show ddos-protection protocols lmpv6
<get-ddos-lmpv6-information>
show ddos-protection protocols lmpv6 aggregate
<get-ddos-lmpv6-aggregate>
show ddos-protection protocols lmpv6 parameters
<get-ddos-lmpv6-parameters>
show ddos-protection protocols lmpv6 statistics
<get-ddos-lmpv6-statistics>
show ddos-protection protocols lmpv6 violations
<get-ddos-lmpv6-violations>
show ddos-protection protocols localnh
  <get-ddos-localnh-information>
show ddos-protection protocols localnh aggregate
  <get-ddos-localnh-aggregate>
show ddos-protection protocols localnh aggregate culprit-flows
  <get-ddos-localnh-aggregate-flows>
show ddos-protection protocols localnh culprit-flows
  <get-ddos-localnh-flows>
show ddos-protection protocols localnh flow-detection
  <get-ddos-localnh-flow-parameters>
show ddos-protection protocols localnh parameters
  <get-ddos-localnh-parameters>
show ddos-protection protocols localnh statistics
  <get-ddos-localnh-statistics>

```

```
show ddos-protection protocols localnh violations
  <get-ddos-localnh-violations>
show ddos-protection protocols mac-host
  <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
  <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host aggregate culprit-flows
  <get-ddos-mac-host-aggregate-flows>
show ddos-protection protocols mac-host culprit-flows
  <get-ddos-mac-host-flows>
show ddos-protection protocols mac-host flow-detection
  <get-ddos-mac-host-flow-parameters>
show ddos-protection protocols mac-host parameters
  <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
  <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
  <get-ddos-mac-host-violations>
show ddos-protection protocols martian-address
  <get-ddos-martian-address-information>
show ddos-protection protocols martian-address aggregate
  <get-ddos-martian-address-aggregate>
show ddos-protection protocols martian-address aggregate culprit-flows
  <get-ddos-martian-address-aggregate-flows>
show ddos-protection protocols martian-address culprit-flows
  <get-ddos-martian-address-flows>
show ddos-protection protocols martian-address flow-detection
  <get-ddos-martian-address-flow-parameters>
show ddos-protection protocols martian-address parameters
  <get-ddos-martian-address-parameters>
show ddos-protection protocols martian-address statistics
  <get-ddos-martian-address-statistics>
show ddos-protection protocols martian-address violations
  <get-ddos-martian-address-violations>
show ddos-protection protocols mac-host
  <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
  <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host parameters
  <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
  <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
  <get-ddos-mac-host-violations>
show ddos-protection protocols mlp
  <get-ddos-mlp-information>
show ddos-protection protocols mlp add
  <get-ddos-mlp-add>
show ddos-protection protocols mlp add culprit-flows
  <get-ddos-mlp-add-flows>
show ddos-protection protocols mlp aggregate
  <get-ddos-mlp-aggregate>
show ddos-protection protocols mlp aging-exception
  <get-ddos-mlp-aging-exc>
show ddos-protection protocols mlp packets
  <get-ddos-mlp-packets>
show ddos-protection protocols mlp parameters
  <get-ddos-mlp-parameters>
show ddos-protection protocols mlp statistics
  <get-ddos-mlp-statistics>
show ddos-protection protocols mlp unclassified
```

```

    <get-ddos-mlp-unclass>
show ddos-protection protocols mlp violations
    <get-ddos-mlp-violations>
show ddos-protection protocols msdp
    <get-ddos-msdp-information>
show ddos-protection protocols msdp aggregate
    <get-ddos-msdp-aggregate>
show ddos-protection protocols msdp parameters
    <get-ddos-msdp-parameters>
show ddos-protection protocols msdp statistics
    <get-ddos-msdp-statistics>
show ddos-protection protocols msdp violations
    <get-ddos-msdp-violations>
show ddos-protection protocols msdpv6
    <get-ddos-msdpv6-information>
show ddos-protection protocols msdpv6 aggregate
    <get-ddos-msdpv6-aggregate>
show ddos-protection protocols msdpv6 parameters
    <get-ddos-msdpv6-parameters>
show ddos-protection protocols msdpv6 statistics
    <get-ddos-msdpv6-statistics>
show ddos-protection protocols msdpv6 violations
    <get-ddos-msdpv6-violations>
show ddos-protection protocols multicast-copy
    <get-ddos-mcast-copy-information>
show ddos-protection protocols multicast-copy aggregate
    <get-ddos-mcast-copy-aggregate>
show ddos-protection protocols multicast-copy parameters
    <get-ddos-mcast-copy-parameters>
show ddos-protection protocols multicast-copy statistics
    <get-ddos-mcast-copy-statistics>
show ddos-protection protocols multicast-copy violations
    <get-ddos-mcast-copy-violations>
show ddos-protection protocols mvrp
    <get-ddos-mvrp-information>
show ddos-protection protocols mvrp aggregate
    <get-ddos-mvrp-aggregate>
show ddos-protection protocols mvrp parameters
    <get-ddos-mvrp-parameters>
show ddos-protection protocols mvrp statistics
    <get-ddos-mvrp-statistics>
show ddos-protection protocols mvrp violations
    <get-ddos-mvrp-violations>
show ddos-protection protocols nonucast-switch
    <get-ddos-nonucast-switch-information>
show ddos-protection protocols nonucast-switch aggregate
    <get-ddos-nonucast-switch-aggregate>
show ddos-protection protocols nonucast-switch aggregate culprit-flows
    <get-ddos-nonucast-switch-aggregate-flows>
show ddos-protection protocols nonucast-switch culprit-flows
    <get-ddos-nonucast-switch-flows>
show ddos-protection protocols nonucast-switch flow-detection
    <get-ddos-nonucast-switch-flow-parameters>
show ddos-protection protocols nonucast-switch parameters
    <get-ddos-nonucast-switch-parameters>
show ddos-protection protocols nonucast-switch statistics
    <get-ddos-nonucast-switch-statistics>
show ddos-protection protocols nonucast-switch violations
    <get-ddos-nonucast-switch-violations>
show ddos-protection protocols ntp
    get-ddos-ntp-information

```

```
show ddos-protection protocols ntp aggregate
  get-ddos-ntp-aggregate
show ddos-protection protocols ntp parameters
  get-ddos-ntp-parameters
show ddos-protection protocols ntp statistics
  get-ddos-ntp-statistics
show ddos-protection protocols ntp violations
  get-ddos-ntp-violations
show ddos-protection protocols oam-lfm
  get-ddos-oam-lfm-information
show ddos-protection protocols oam-lfm aggregate
  get-ddos-oam-lfm-aggregate
show ddos-protection protocols oam-lfm parameters
  get-ddos-oam-lfm-parameters
show ddos-protection protocols oam-lfm statistics
  get-ddos-oam-lfm-statistics
show ddos-protection protocols oam-lfm violations
  get-ddos-oam-lfm-violations
show ddos-protection protocols ospf
  get-ddos-ospf-information
show ddos-protection protocols ospf aggregate
  get-ddos-ospf-aggregate
show ddos-protection protocols ospf parameters
  get-ddos-ospf-parameters
show ddos-protection protocols ospf statistics
  get-ddos-ospf-statistics
show ddos-protection protocols ospf violations
  get-ddos-ospf-violations
show ddos-protection protocols ospf-hello
  <get-ddos-ospf-hello-information>
show ddos-protection protocols ospf-hello aggregate
  <get-ddos-ospf-hello-aggregate>
show ddos-protection protocols ospf-hello aggregate culprit-flows
  <get-ddos-ospf-hello-aggregate-flows>
show ddos-protection protocols ospf-hello culprit-flows
  <get-ddos-ospf-hello-flows>
show ddos-protection protocols ospf-hello flow-detection
  <get-ddos-ospf-hello-flow-parameters>
show ddos-protection protocols ospf-hello parameters
  <get-ddos-ospf-hello-parameters>
show ddos-protection protocols ospf-hello statistics
  <get-ddos-ospf-hello-statistics>
show ddos-protection protocols ospf-hello violations
  <get-ddos-ospf-hello-violations>
show ddos-protection protocols ospfv3v6
  get-ddos-ospfv3v6-information
show ddos-protection protocols ospfv3v6 aggregate
  get-ddos-ospfv3v6-aggregate
show ddos-protection protocols ospfv3v6 parameters
  get-ddos-ospfv3v6-parameters
show ddos-protection protocols ospfv3v6 statistics
  get-ddos-ospfv3v6-statistics
show ddos-protection protocols ospfv3v6 violations
  get-ddos-ospfv3v6-violations
show ddos-protection protocols parameters
  get-ddos-protocols-parameters
show ddos-protection protocols pfe-alive
  get-ddos-pfe-alive-information
show ddos-protection protocols pfe-alive aggregate
  get-ddos-pfe-alive-aggregate
show ddos-protection protocols pfe-alive parameters
```

```
get-ddos-pfe-alive-parameters
show ddos-protection protocols pfe-alive statistics
get-ddos-pfe-alive-statistics
show ddos-protection protocols pfe-alive violations
get-ddos-pfe-alive-violations
show ddos-protection protocols pim
get-ddos-pim-information
show ddos-protection protocols pim aggregate
get-ddos-pim-aggregate
show ddos-protection protocols pim aggregate culprit-flows
show ddos-protection protocols pim parameters
get-ddos-pim-parameters
show ddos-protection protocols pim statistics
get-ddos-pim-statistics
show ddos-protection protocols pim violations
get-ddos-pim-violations
show ddos-protection protocols pim-ctrl
<get-ddos-pim-ctrl-information>
show ddos-protection protocols pim-ctrl aggregate
<get-ddos-pim-ctrl-aggregate>
show ddos-protection protocols pim-ctrl aggregate culprit-flows
<get-ddos-pim-ctrl-aggregate-flows>
show ddos-protection protocols pim-ctrl culprit-flows
<get-ddos-pim-ctrl-flows>
show ddos-protection protocols pim-ctrl flow-detection
<get-ddos-pim-ctrl-flow-parameters>
show ddos-protection protocols pim-ctrl parameters
<get-ddos-pim-ctrl-parameters>
show ddos-protection protocols pim-ctrl statistics
<get-ddos-pim-ctrl-statistics>
show ddos-protection protocols pim-ctrl violations
<get-ddos-pim-ctrl-violations>
show ddos-protection protocols pim-data
<get-ddos-pim-data-information>
show ddos-protection protocols pim-data aggregate
<get-ddos-pim-data-aggregate>
show ddos-protection protocols pim-data aggregate culprit-flows
<get-ddos-pim-data-aggregate-flows>
show ddos-protection protocols pim-data culprit-flows
<get-ddos-pim-data-flows>
show ddos-protection protocols pim-data flow-detection
<get-ddos-pim-data-flow-parameters>
show ddos-protection protocols pim-data parameters
<get-ddos-pim-data-parameters>
show ddos-protection protocols pim-data statistics
<get-ddos-pim-data-statistics>
show ddos-protection protocols pim-data violations
<get-ddos-pim-data-violations>
show ddos-protection protocols pimv6
<get-ddos-pimv6-information>
show ddos-protection protocols pimv6 aggregate
<get-ddos-pimv6-aggregate>
show ddos-protection protocols pimv6 aggregate culprit-flows
show ddos-protection protocols pimv6 parameters
<get-ddos-pimv6-parameters>
show ddos-protection protocols pimv6 statistics
<get-ddos-pimv6-statistics>
show ddos-protection protocols pimv6 violations
<get-ddos-pimv6-violations>
```

```
show ddos-protection protocols pmvrp
  get-ddos-pmvrp-information
show ddos-protection protocols pmvrp aggregate
  get-ddos-pmvrp-aggregate
show ddos-protection protocols pmvrp parameters
  get-ddos-pmvrp-parameters
show ddos-protection protocols pmvrp statistics
  get-ddos-pmvrp-statistics
show ddos-protection protocols pmvrp violations
  get-ddos-pmvrp-violations
show ddos-protection protocols pos
  get-ddos-pos-information
show ddos-protection protocols pos aggregate
  get-ddos-pos-aggregate
show ddos-protection protocols pos aggregate culprit-flows
show ddos-protection protocols pos parameters
  get-ddos-pos-parameters
show ddos-protection protocols pos statistics
  get-ddos-pos-statistics
show ddos-protection protocols pos violations
  get-ddos-pos-violations
show ddos-protection protocols ppp
  get-ddos-ppp-information
show ddos-protection protocols ppp aggregate
  get-ddos-ppp-aggregate
show ddos-protection protocols ppp authentication
  get-ddos-ppp-auth
show ddos-protection protocols ppp authentication culprit-flows
show ddos-protection protocols ppp ipcp
  get-ddos-ppp-ipcp
show ddos-protection protocols ppp ipv6cp
  get-ddos-ppp-ipv6cp
show ddos-protection protocols ppp isis
  get-ddos-ppp-isis
show ddos-protection protocols ppp isis culprit-flows
show ddos-protection protocols ppp lcp
  get-ddos-ppp-lcp
show ddos-protection protocols ppp lcp culprit-flows
show ddos-protection protocols ppp mplsdp
  get-ddos-ppp-mplsdp
show ddos-protection protocols ppp mplsdp culprit-flows
show ddos-protection protocols ppp parameters
  get-ddos-ppp-parameters
show ddos-protection protocols ppp statistics
  get-ddos-ppp-statistics
show ddos-protection protocols ppp unclassified
<get-ddos-ppp-unclass>
show ddos-protection protocols ppp violations
  get-ddos-ppp-violations
show ddos-protection protocols pppoe
  get-ddos-pppoe-information
show ddos-protection protocols pppoe aggregate
  get-ddos-pppoe-aggregate
show ddos-protection protocols pppoe padi
  get-ddos-pppoe-padi
show ddos-protection protocols pppoe padm
  get-ddos-pppoe-padm
show ddos-protection protocols pppoe padn
  get-ddos-pppoe-padn
show ddos-protection protocols pppoe pado
  get-ddos-pppoe-pado
```



```

show ddos-protection protocols pppoe padr
  get-ddos-pppoe-padr
show ddos-protection protocols pppoe pads
  get-ddos-pppoe-pads
show ddos-protection protocols pppoe padt
  get-ddos-pppoe-padt
show ddos-protection protocols pppoe parameters
  get-ddos-pppoe-parameters
show ddos-protection protocols pppoe statistics
  get-ddos-pppoe-statistics
show ddos-protection protocols pppoe violations
  get-ddos-pppoe-violations
show ddos-protection protocols ptp
  get-ddos-ntp-information
show ddos-protection protocols ptp aggregate
  get-ddos-ntp-aggregate
show ddos-protection protocols ptp aggregate culprit-flows
show ddos-protection protocols ptp parameters
  get-ddos-ntp-parameters
show ddos-protection protocols ptp statistics
  get-ddos-ntp-statistics
show ddos-protection protocols ptp violations
  get-ddos-ntp-violations
show ddos-protection protocols pvstp
  get-ddos-pvstp-information
show ddos-protection protocols pvstp aggregate
  get-ddos-pvstp-aggregate
show ddos-protection protocols pvstp parameters
  get-ddos-pvstp-parameters
show ddos-protection protocols pvstp statistics
  get-ddos-pvstp-statistics
show ddos-protection protocols pvstp violations
  get-ddos-pvstp-violations
show ddos-protection protocols radius
  get-ddos-radius-information
show ddos-protection protocols radius accounting
  get-ddos-radius-account
show ddos-protection protocols radius aggregate
  get-ddos-radius-aggregate
show ddos-protection protocols radius accounting culprit-flows
show ddos-protection protocols radius authorization
  get-ddos-radius-auth
show ddos-protection protocols radius parameters
  get-ddos-radius-parameters
show ddos-protection protocols radius server
  get-ddos-radius-server
show ddos-protection protocols radius statistics
  get-ddos-radius-statistics
show ddos-protection protocols radius violations
  get-ddos-radius-violations
show ddos-protection protocols re-services
  <get-ddos-re-services-information>
show ddos-protection protocols re-services aggregate
  <get-ddos-re-services-aggregate>
show ddos-protection protocols re-services aggregate culprit-flows
  <get-ddos-re-services-aggregate-flows>
show ddos-protection protocols re-services captive-portal
  <get-ddos-re-services-captive-portal>
show ddos-protection protocols re-services captive-portal culprit-flows
  <get-ddos-re-services-captive-portal-flows>
show ddos-protection protocols re-services culprit-flows

```

```
<get-ddos-re-services-flows>
show ddos-protection protocols re-services flow-detection
  <get-ddos-re-services-flow-parameters>
show ddos-protection protocols re-services parameters
  <get-ddos-re-services-parameters>
show ddos-protection protocols re-services statistics
  <get-ddos-re-services-statistics>
show ddos-protection protocols re-services violations
  <get-ddos-re-services-violations>
show ddos-protection protocols re-services-v6
  <get-ddos-re-services-v6-information>
show ddos-protection protocols re-services-v6 aggregate
  <get-ddos-re-services-v6-aggregate>
show ddos-protection protocols re-services-v6 aggregate culprit-flows
  <get-ddos-re-services-v6-aggregate-flows>
show ddos-protection protocols re-services-v6 captive-portal
  <get-ddos-re-services-v6-captive-portal-v6>
show ddos-protection protocols re-services-v6 captive-portal culprit-flows
  <get-ddos-re-services-v6-captive-portal-v6-flows>
show ddos-protection protocols re-services-v6 culprit-flows
  <get-ddos-re-services-v6-flows>
show ddos-protection protocols re-services-v6 flow-detection
  <get-ddos-re-services-v6-flow-parameters>
show ddos-protection protocols re-services-v6 parameters
  <get-ddos-re-services-v6-parameters>
show ddos-protection protocols re-services-v6 statistics
  <get-ddos-re-services-v6-statistics>
show ddos-protection protocols re-services-v6 violations
  <get-ddos-re-services-v6-violations>
show ddos-protection protocols redirect
  get-ddos-redirect-information
show ddos-protection protocols redirect aggregate
  get-ddos-redirect-aggregate
show ddos-protection protocols redirect parameters
  get-ddos-redirect-parameters
show ddos-protection protocols redirect statistics
  get-ddos-redirect-statistics
show ddos-protection protocols redirect violations
  get-ddos-redirect-violations

show ddos-protection protocols reject
  <get-ddos-reject-information>
show ddos-protection protocols reject aggregate
  <get-ddos-reject-aggregate>
show ddos-protection protocols reject parameters
  <get-ddos-reject-parameters>
show ddos-protection protocols reject statistics
  <get-ddos-reject-statistics>
show ddos-protection protocols reject violations
  <get-ddos-reject-violations>
show ddos-protection protocols rejectv6show ddos-protection protocols rejectv6
  aggregate
show ddos-protection protocols rejectv6 aggregate culprit-flows
show ddos-protection protocols rejectv6 flow-detection
show ddos-protection protocols rejectv6 parameters
show ddos-protection protocols rejectv6 statistics
show ddos-protection protocols rejectv6 violations
show ddos-protection protocols rip
  get-ddos-rip-information
show ddos-protection protocols rip aggregate
```

```

get-ddos-rip-aggregate
show ddos-protection protocols rip aggregate culprit-flows
show ddos-protection protocols rip culprit-flows
show ddos-protection protocols rip parameters
get-ddos-rip-parameters
show ddos-protection protocols rip statistics
get-ddos-rip-statistics
show ddos-protection protocols rip violations
get-ddos-rip-violations
show ddos-protection protocols ripv6
get-ddos-ripv6-information
show ddos-protection protocols ripv6 aggregate
get-ddos-ripv6-aggregate
show ddos-protection protocols ripv6 aggregate culprit-flows
show ddos-protection protocols ripv6 parameters
get-ddos-ripv6-parameters
show ddos-protection protocols ripv6 statistics
get-ddos-ripv6-statistics
show ddos-protection protocols ripv6 violations
get-ddos-ripv6-violations
show ddos-protection protocols rsvp
get-ddos-rsvp-information
show ddos-protection protocols rsvp aggregate
get-ddos-rsvp-aggregate
show ddos-protection protocols rsvp aggregate culprit-flows
show ddos-protection protocols rsvp parameters
get-ddos-rsvp-parameters
show ddos-protection protocols rsvp statistics
get-ddos-rsvp-statistics
show ddos-protection protocols rsvp violations
get-ddos-rsvp-violations
show ddos-protection protocols rsvpv6
get-ddos-rsvpv6-information
show ddos-protection protocols rsvpv6 aggregate
get-ddos-rsvpv6-aggregate
show ddos-protection protocols rsvpv6 aggregate culprit-flows
show ddos-protection protocols rsvpv6 parameters
get-ddos-rsvpv6-parameters
show ddos-protection protocols rsvpv6 statistics
get-ddos-rsvpv6-statistics
show ddos-protection protocols rsvpv6 violations
get-ddos-rsvpv6-violations
show ddos-protection protocols sample
<get-ddos-sample-information>
show ddos-protection protocols sample aggregate
<get-ddos-sample-aggregate>
show ddos-protection protocols sample aggregate culprit-flows
show ddos-protection protocols sample host
<get-ddos-sample-host>
show ddos-protection protocols sample parameters
<get-ddos-sample-parameters>
show ddos-protection protocols sample pfe
<get-ddos-sample-pfe>
show ddos-protection protocols sample pfe culprit-flows
show ddos-protection protocols sample sflow
<get-ddos-sample-sflow>
show ddos-protection protocols sample sflow culprit-flows
<get-ddos-sample-sflow-flows>
show ddos-protection protocols sample statistics
<get-ddos-sample-statistics>
show ddos-protection protocols sample syslog

```

```
show ddos-protection protocols sample tap
<get-ddos-sample-tap>
show ddos-protection protocols sample tap culprit-flows
show ddos-protection protocols sample violations
<get-ddos-sample-violations>
show ddos-protection protocols services
  get-ddos-services-information
show ddos-protection protocols sample-dest
<get-ddos-sample-dest-information>
show ddos-protection protocols sample-dest aggregate
<get-ddos-sample-dest-aggregate>
show ddos-protection protocols sample-dest aggregate culprit-flows
<get-ddos-sample-dest-aggregate-flows>
show ddos-protection protocols sample-dest culprit-flows
<get-ddos-sample-dest-flows>
show ddos-protection protocols sample-dest flow-detection
<get-ddos-sample-dest-flow-parameters>
show ddos-protection protocols sample-dest parameters
<get-ddos-sample-dest-parameters>
show ddos-protection protocols sample-dest statistics
<get-ddos-sample-dest-statistics>
show ddos-protection protocols sample-dest violations
<get-ddos-sample-dest-violations>
show ddos-protection protocols sample-source
<get-ddos-sample-source-information>
show ddos-protection protocols sample-source aggregate
<get-ddos-sample-source-aggregate>
show ddos-protection protocols sample-source aggregate culprit-flows
<get-ddos-sample-source-aggregate-flows>
show ddos-protection protocols sample-source culprit-flows
<get-ddos-sample-source-flows>
show ddos-protection protocols sample-source flow-detection
<get-ddos-sample-source-flow-parameters>
show ddos-protection protocols sample-source parameters
<get-ddos-sample-source-parameters>
show ddos-protection protocols sample-source statistics
<get-ddos-sample-source-statistics>
show ddos-protection protocols sample-source violations
<get-ddos-sample-source-violations>
show ddos-protection protocols services aggregate
  <get-ddos-services-aggregate>
show ddos-protection protocols services parameters
  <get-ddos-services-parameters>
show ddos-protection protocols services statistics
  <get-ddos-services-statistics>
show ddos-protection protocols syslog
  <get-ddos-syslog-information>
show ddos-protection protocols syslog aggregate
  <get-ddos-syslog-aggregate>
show ddos-protection protocols syslog aggregate culprit-flows
  <get-ddos-syslog-aggregate-flows>
show ddos-protection protocols syslog culprit-flows
  <get-ddos-syslog-flows>
show ddos-protection protocols syslog flow-detection
  <get-ddos-syslog-flow-parameters>
show ddos-protection protocols syslog parameters
  <get-ddos-syslog-parameters>
show ddos-protection protocols syslog statistics
  <get-ddos-syslog-statistics>
show ddos-protection protocols syslog violations
  <get-ddos-syslog-violations>
```

```
show ddos-protection protocols services violations
  get-ddos-services-violations
show ddos-protection protocols snmp
  get-ddos-snmp-information
show ddos-protection protocols snmp aggregate
  get-ddos-snmp-aggregate
show ddos-protection protocols snmp aggregate culprit-flows
show ddos-protection protocols snmp parameters
  get-ddos-snmp-parameters
show ddos-protection protocols snmp statistics
  get-ddos-snmp-statistics
show ddos-protection protocols snmp violations
  get-ddos-snmp-violations
show ddos-protection protocols snmpv6
  get-ddos-snmpv6-information
show ddos-protection protocols snmpv6 aggregate
  get-ddos-snmpv6-aggregate
show ddos-protection protocols snmpv6 aggregate culprit-flows
show ddos-protection protocols snmpv6 parameters
  get-ddos-snmpv6-parameters
show ddos-protection protocols snmpv6 statistics
  get-ddos-snmpv6-statistics
show ddos-protection protocols snmpv6 violations
  get-ddos-snmpv6-violations
show ddos-protection protocols ssh
  get-ddos-ssh-information
show ddos-protection protocols ssh aggregate
  get-ddos-ssh-aggregate
show ddos-protection protocols ssh parameters
  get-ddos-ssh-parameters
show ddos-protection protocols ssh statistics
  get-ddos-ssh-statistics
show ddos-protection protocols ssh violations
  get-ddos-ssh-violations
show ddos-protection protocols sshv6
  get-ddos-sshv6-information
show ddos-protection protocols sshv6 aggregate
  get-ddos-sshv6-aggregate
show ddos-protection protocols sshv6 parameters
  get-ddos-sshv6-parameters
show ddos-protection protocols sshv6 statistics
  <get-ddos-sshv6-statistics>
show ddos-protection protocols sshv6 violations
  <get-ddos-sshv6-violations>
show ddos-protection protocols statistics
  <get-ddos-protocols-statistics>
show ddos-protection protocols stp
  <get-ddos-stp-information>
show ddos-protection protocols stp aggregate
  <get-ddos-stp-aggregate>
show ddos-protection protocols stp parameters
  <get-ddos-stp-parameters>
show ddos-protection protocols stp statistics
  <get-ddos-stp-statistics>
show ddos-protection protocols stp violations
  <get-ddos-stp-violations>
show ddos-protection protocols tacacs
  <get-ddos-tacacs-information>
show ddos-protection protocols tacacs aggregate
  <get-ddos-tacacs-aggregate>
show ddos-protection protocols tacacs parameters
```

```
<get-ddos-tacacs-parameters>
show ddos-protection protocols tacacs statistics
<get-ddos-tacacs-statistics>
show ddos-protection protocols tacacs violations
<get-ddos-tacacs-violations>
show ddos-protection protocols tcp-flags
<get-ddos-tcp-flags-information>
show ddos-protection protocols tcp-flags aggregate
<get-ddos-tcp-flags-aggregate>
show ddos-protection protocols tcp-flags established
<get-ddos-tcp-flags-establish>
show ddos-protection protocols tcp-flags initial
<get-ddos-tcp-flags-initial>
show ddos-protection protocols tcp-flags parameters
<get-ddos-tcp-flags-parameters>
show ddos-protection protocols tcp-flags statistics
<get-ddos-tcp-flags-statistics>
show ddos-protection protocols tcp-flags unclassified
<get-ddos-tcp-flags-unclass>
show ddos-protection protocols tcp-flags violations
<get-ddos-tcp-flags-violations>
show ddos-protection protocols telnet
<get-ddos-telnet-information>
show ddos-protection protocols telnet aggregate
<get-ddos-telnet-aggregate>
show ddos-protection protocols telnet aggregate culprit-flows
show ddos-protection protocols telnet parameters
<get-ddos-telnet-parameters>
show ddos-protection protocols telnet statistics
<get-ddos-telnet-statistics>
show ddos-protection protocols telnet violations
<get-ddos-telnet-violations>
show ddos-protection protocols telnetv6
<get-ddos-telnetv6-information>
show ddos-protection protocols telnetv6 aggregate
<get-ddos-telnetv6-aggregate>
show ddos-protection protocols telnetv6 aggregate culprit-flows
show ddos-protection protocols telnetv6 parameters
<get-ddos-telnetv6-parameters>
show ddos-protection protocols telnetv6 statistics
<get-ddos-telnetv6-statistics>
show ddos-protection protocols telnetv6 violations
<get-ddos-telnetv6-violations>
show ddos-protection protocols ttl
<get-ddos-ttl-information>
show ddos-protection protocols ttl aggregate
<get-ddos-ttl-aggregate>
show ddos-protection protocols ttl parameters
<get-ddos-ttl-parameters>
show ddos-protection protocols ttl statistics
<get-ddos-ttl-statistics>
show ddos-protection protocols ttl violations
<get-ddos-ttl-violations>
show ddos-protection protocols tunnel-fragment
<get-ddos-tun-frag-information>
show ddos-protection protocols tunnel-fragment aggregate
<get-ddos-tun-frag-aggregate>
show ddos-protection protocols tunnel-fragment aggregate culprit-flows
show ddos-protection protocols tunnel-fragment parameters
<get-ddos-tun-frag-parameters>
show ddos-protection protocols tunnel-fragment statistics
```

```

    <get-ddos-tun-frag-statistics>
show ddos-protection protocols tunnel-fragment violations
    <get-ddos-tun-frag-violations>
show ddos-protection protocols tunnel-ka
    <get-ddos-tunnel-ka-information>
show ddos-protection protocols tunnel-ka aggregate
    <get-ddos-tunnel-ka-aggregate>
show ddos-protection protocols tunnel-ka aggregate culprit-flows
    <get-ddos-tunnel-ka-aggregate-flows>
show ddos-protection protocols tunnel-ka culprit-flows
    <get-ddos-tunnel-ka-flows>
show ddos-protection protocols tunnel-ka flow-detection
    <get-ddos-tunnel-ka-flow-parameters>
show ddos-protection protocols tunnel-ka parameters
    <get-ddos-tunnel-ka-parameters>
show ddos-protection protocols tunnel-ka statistics
    <get-ddos-tunnel-ka-statistics>
show ddos-protection protocols tunnel-ka violations
    <get-ddos-tunnel-ka-violations>
show ddos-protection protocols unknown-l2mc
    <get-ddos-unknown-l2mc-information>
show ddos-protection protocols unknown-l2mc aggregate
    <get-ddos-unknown-l2mc-aggregate>
show ddos-protection protocols unknown-l2mc aggregate culprit-flows
    <get-ddos-unknown-l2mc-aggregate-flows>
show ddos-protection protocols unknown-l2mc culprit-flows
    <get-ddos-unknown-l2mc-flows>
show ddos-protection protocols unknown-l2mc flow-detection
    <get-ddos-unknown-l2mc-flow-parameters>
show ddos-protection protocols unknown-l2mc parameters
    <get-ddos-unknown-l2mc-parameters>
show ddos-protection protocols unknown-l2mc statistics
    <get-ddos-unknown-l2mc-statistics>
show ddos-protection protocols unknown-l2mc violations
    <get-ddos-unknown-l2mc-violations>
show ddos-protection protocols unclassified
<get-ddos-uncls-information>
show ddos-protection protocols unclassified aggregate
<get-ddos-uncls-aggregate>
show ddos-protection protocols unclassified parameters
<get-ddos-uncls-parameters>
show ddos-protection protocols unclassified resolve-v4
show ddos-protection protocols unclassified resolve-v4 culprit-flows
show ddos-protection protocols unclassified resolve-v6
show ddos-protection protocols unclassified resolve-v6 culprit-flows
show ddos-protection protocols unclassified statistics
<get-ddos-uncls-statistics>
show ddos-protection protocols unclassified violations
<get-ddos-uncls-violations>
show ddos-protection protocols urpf-fail
    <get-ddos-urpf-fail-information>
show ddos-protection protocols urpf-fail aggregate
    <get-ddos-urpf-fail-aggregate>
show ddos-protection protocols urpf-fail aggregate culprit-flows
    <get-ddos-urpf-fail-aggregate-flows>
show ddos-protection protocols urpf-fail culprit-flows
    <get-ddos-urpf-fail-flows>
show ddos-protection protocols urpf-fail flow-detection
    <get-ddos-urpf-fail-flow-parameters>
show ddos-protection protocols urpf-fail parameters
    <get-ddos-urpf-fail-parameters>

```

```
show ddos-protection protocols urpf-fail statistics
  <get-ddos-urpf-fail-statistics>
show ddos-protection protocols urpf-fail violations
  <get-ddos-urpf-fail-violations>
show ddos-protection protocols vcipc-udp
  <get-ddos-vcipc-udp-information>
show ddos-protection protocols vcipc-udp aggregate
  <get-ddos-vcipc-udp-aggregate>
show ddos-protection protocols vcipc-udp aggregate culprit-flows
  <get-ddos-vcipc-udp-aggregate-flows>
show ddos-protection protocols vcipc-udp culprit-flows
  <get-ddos-vcipc-udp-flows>
show ddos-protection protocols vcipc-udp flow-detection
  <get-ddos-vcipc-udp-flow-parameters>
show ddos-protection protocols vcipc-udp parameters
  <get-ddos-vcipc-udp-parameters>
show ddos-protection protocols vcipc-udp statistics
  <get-ddos-vcipc-udp-statistics>
show ddos-protection protocols vcipc-udp violations
  <get-ddos-vcipc-udp-violations>
show ddos-protection protocols violations
  get-ddos-protocols-violations
show ddos-protection protocols virtual-chassis
  get-ddos-vchassis-information
show ddos-protection protocols virtual-chassis aggregate
  get-ddos-vchassis-aggregate
show ddos-protection protocols virtual-chassis aggregate culprit-flows
show ddos-protection protocols virtual-chassis control-high
  get-ddos-vchassis-control-hi
show ddos-protection protocols virtual-chassis control-low
  get-ddos-vchassis-control-lo
show ddos-protection protocols virtual-chassis parameters
  get-ddos-vchassis-parameters
show ddos-protection protocols virtual-chassis statistics
  get-ddos-vchassis-statistics
show ddos-protection protocols virtual-chassis unclassified
  get-ddos-vchassis-unclass
show ddos-protection protocols virtual-chassis vc-packets
  get-ddos-vchassis-vc-packets
show ddos-protection protocols virtual-chassis vc-ttl-errors
  get-ddos-vchassis-vc-ttl-err
show ddos-protection protocols virtual-chassis violations
  get-ddos-vchassis-violations
show ddos-protection protocols vrrp
  get-ddos-vrrp-information
show ddos-protection protocols vrrp aggregate
  get-ddos-vrrp-aggregate
show ddos-protection protocols vrrp aggregate culprit-flows
show ddos-protection protocols vrrp parameters
  get-ddos-vrrp-parameters
show ddos-protection protocols vrrp statistics
  get-ddos-vrrp-statistics
show ddos-protection protocols vrrp violations
  get-ddos-vrrp-violations
show ddos-protection protocols vrrpv6
  get-ddos-vrrpv6-information
show ddos-protection protocols vrrpv6 aggregate
  get-ddos-vrrpv6-aggregate
show ddos-protection protocols vrrpv6 aggregate culprit-flows
show ddos-protection protocols vrrpv6 parameters
  get-ddos-vrrpv6-parameters
```



```
show ddos-protection protocols vrrpv6 statistics
  get-ddos-vrrpv6-statistics
show ddos-protection protocols vrrpv6 violations
  get-ddos-vrrpv6-violations
show ddos-protection statistics
  get-ddos-statistics-information
show ddos-protection version
  get-ddos-version
show ddos-protection protocols vxlan
  <get-ddos-vxlan-information>
show ddos-protection protocols vxlan aggregate
  <get-ddos-vxlan-aggregate>
show ddos-protection protocols vxlan aggregate culprit-flows
  <get-ddos-vxlan-aggregate-flows>
show ddos-protection protocols vxlan culprit-flows
  <get-ddos-vxlan-flows>
show ddos-protection protocols vxlan flow-detection
  <get-ddos-vxlan-flow-parameters>
show ddos-protection protocols vxlan parameters
  <get-ddos-vxlan-parameters>
show ddos-protection protocols vxlan statistics
  <get-ddos-vxlan-statistics>
show ddos-protection protocols vxlan violations
  <get-ddos-vxlan-violations>

show dhcp
show dhcp proxy-client
show dhcp proxy-client binding
show dhcp proxy-client servers
show dhcp proxy-client statistics
  <get-proxy-dhcp-client-statistics-information>
show dhcp relay
show dhcp relay binding
  <get-dhcp-relay-binding-information>

show dhcp relay binding interface
  <get-dhcp-relay-interface-bindings>
show dhcp relay binding lease-time-violation
  <get-dhcp-relay-binding-ltv-information>
show dhcp relay statistics
  <get-dhcp-relay-statistics-information>
show dhcp relay statistics bulk-leasequery-connections
  <get-dhcp-relay-bulk-leasequery-conn-statistics>
show dhcp relay statistics leasequery
  <get-dhcp-relay-leasequery-statistics>

show dhcp server
show dhcp server binding
  <get-dhcp-server-binding-information>

show dhcp server binding interface
  <get-dhcp-relay-binding-interface>
show dhcp server binding lease-time-violation
  <get-dhcp-server-binding-ltv-information>
show dhcp server statistics
  <get-dhcp-server-statistics-information>
show dhcp statistics
  <get-dhcp-service-statistics-information>
show dhcpv6

show dhcpv6 proxy-client
show dhcpv6 proxy-client binding
```

```
show dhcpv6 proxy-client statistics
  <get-proxy-dhcpv6-client-statistics-information>
show dhcpv6 relay
show dhcpv6 relay binding
  <get-dhcpv6-relay-binding-information>
show dhcpv6 relay binding interface
  <get-dhcpv6-relay-binding-interface>
show dhcpv6 relay binding lease-time-violation
  <get-dhcpv6-relay-binding-ltv-information>
show dhcpv6 relay statistics
  <get-dhcpv6-relay-statistics-information>
show dhcpv6 relay statistics bulk-leasequery-connections
  <get-dhcpv6-relay-bulk-leasequery-conn-statistics>
show dhcpv6 relay statistics leasequery
  <get-dhcpv6-relay-leasequery-statistics>
show dhcpv6 server
show dhcpv6 server binding
  <get-dhcpv6-server-binding-information>

show dhcpv6 server binding interface
  <get-dhcpv6-server-binding-interface>
show dhcpv6 server binding lease-time-violation
  <get-dhcpv6-server-binding-ltv-information>
show dhcpv6 server statistics
  <get-dhcpv6-server-statistics-information>
show dhcpv6 server statistics bulk-leasequery-connections
  <get-dhcpv6-server-bulk-leasequery-conn-statistics>
show dhcpv6 statistics
  <get-dhcpv6-service-statistics-information>
show diagnostics
show diagnostics tdr
  <get-tdr-interface-information>
show diagnostics tdr interface
  <get-tdr-interface-status>
show diameter
  <get-diameter-information>
show diameter function
  <get-diameter-function-information>
show diameter function statistics
  <get-diameter-function-statistics>
show diameter instance
  <get-diameter-instance-information>
show diameter network-element
  <get-diameter-network-element-information>
show diameter network-element map
  <get-diameter-network-element-map-information>
show diameter peer
  <get-diameter-peer-information>
show diameter peer map
  <get-diameter-peer-map-information>
show diameter peer statistics
  <get-diameter-peer-statistics>
show diameter route
  <get-diameter-route-information>
show dot1x
show dot1x authentication-failed-users
  <get-dot1x-authentication-failed-users>
show dot1x interface
  <get-dot1x-interface-information>
show dot1x static-mac-address
  <get-dot1x-static-mac-addresses>
```

```

show dot1x static-mac-address interface
    <get-dot1x-interface-mac-addresses>
show dvmrp
show dvmrp interfaces
    <get-dvmrp-interfaces-information>
show dvmrp neighbors
    <get-dvmrp-neighbors-information>
show dvmrp prefix
    <get-dvmrp-prefix-information>
show dvmrp prunes
    <get-dvmrp-prunes-information>
show dynamic-profile
    <get-dynamic-profile>
show dynamic-profile session
    <get-dynamic-profile-session-information>
show dynamic-tunnels
show dynamic-tunnels database
    <get-dynamic-tunnels-database>
show ethernet-switching mac-learning-log
    <get-ethernet-switching-log-information>
show ethernet-switching mac-notification
    <get-ethernet-switching-mac-notification-information>
show ethernet-switching vxlan-tunnel-end-point remote vtep-source-interface
    <get-ethernet-switching-vxlan-remote-svtep-ip-information>
show ethernet-switching vxlan-tunnel-end-point source ip
    <get-ethernet-switching-vxlan-svtep-ip-information>
show ephemeral-configuration
show esis
show esis adjacency
    <get-esis-adjacency-information>
show esis interface
    <get-esis-interface-information>
show esis statistics
    <get-esis-statistics-information>
show event-options
show event-options event-scripts
show event-options event-scripts policies
    <get-event-scripts-policies>
<get-event-summary>
show evpn
show evpn arp-table
    <get-evpn-arp-table>
show evpn flood
    <get-evpn-flood-information>
show evpn flood event-queue
    <get-evpn-event-queue-information>
show evpn flood route
show evpn flood route all-ce-flood
    <get-evpn-all-ce-flood-route-information>
show evpn flood route all-flood
    <get-evpn-all-flood-route-information>
show evpn flood route alt-root-flood
    <get-evpn-alt-root-flood-route-information>
show evpn flood route ce-flood
    <get-evpn-ce-flood-route-information>
show evpn flood route mlp-flood
    <get-evpn-mlp-flood-route-information>
show evpn flood route re-flood
    <get-evpn-re-flood-route-information>
show evpn instance
    <get-evpn-instance-information>

```

```
show evpn mac-table
<get-evpn-mac-table>
show evpn mac-table interface
<get-evpn-interface-mac-table>
show evpn peer-gateway-macs
<get-evpn-peer-gateway-mac>
show evpn statistics
<get-evpn-statistics-information>
show extensible-subscriber-services
show extensible-subscriber-services accounting
<get-extensible-subscriber-services-accounting>
show extensible-subscriber-services counters
<get-extensible-subscriber-services-counters>
show extensible-subscriber-services dictionary
<get-extensible-subscriber-services-dictionary>
show extensible-subscriber-services services
<get-extensible-subscriber-services-services>
show extensible-subscriber-services sessions
<get-extensible-subscriber-services-sessions>
show extension-provider
show extension-provider system
show extension-provider system connections
<get-mspinfo-connections>
show extension-provider system packages
<get-mspinfo-packages>
show extension-provider system processes
<get-mspinfo-processes>
show extension-provider system processes brief
<get-mspinfo-processes-brief>
show extension-provider system processes extensive
<get-mspinfo-processes-extensive>
show extension-provider system uptime
<get-mspinfo-uptime>
show extension-provider system virtual-memory
<get-core-key-list>
<get-fabric-summary-information>
<get-key-vg-binding>
<get-mac-ip-binding-information>
<get-mc-ccpc-cache-ccpc-select>
<get-mc-ccpc-cache-root-candidates>
<get-mc-ccpc-cache-spf>
<get-mc-ccpc-src-mod-filters>
<get-mc-edge-cache-ccpc-select>
<get-mc-edge-map-to-key-binding>
<get-mc-edge-key-to-map-binding>
<get-mc-edge-vg-portmap>
<get-mc-nsf>
<get-mc-root-cache-trunk>
<get-mc-root-key-to-map-binding>
<get-layer2-group-membership-entries>
<get-layer3-group-membership-entries>
<get-layer3-multicast-pending-routes>
<get-layer3-multicast-receivers>
<get-mc-root-map-to-key-binding>
<get-mc-root-vg-pfemap>
<get-fabric-multicast-statistics>
<get-mc-vccpdf-adjacency-database>
<get-mspinfo-virtual-memory>
get-fabric-statistics
get-fabric-summary-information
<get-vlan-domain-map-information>
```

```
show fabric multicast dirty-key-info
<get-mc-dirty-key-info>
show fabric multicast edge corekey-ifls-filters
<get-mc-edge-corekey-ifls-filters>
show fabric multicast edge ine-ifls-filters
<get-mc-edge-ine-ifls-filters>
show fabric multicast edge src-mod-filters
<get-mc-edge-src-mod-filters>
show fabric multicast graph
show fabric multicast graph core-tree
<get-fabric-multicast-graph>
show fabric multicast steal-key-info
<get-mc-steal-key-info>
show forwarding-options
show forwarding-options enhanced-hash-key
show forwarding-options enhanced-hash-key fpc
show forwarding-options hyper-mode
<get forwarding-options hyper-mode>
show forwarding-options next-hop-group
<get-forwarding-options-next-hop-group>
show forwarding-options port-mirroring
<get-forwarding-options-port-mirroring>
show helper
show helper statistics
    <get-helper-statistics-information>
show hfrr
show hfrr profiles
show iccp
    <get-inter-chassis-control-protocol-information>
show igmp
show igmp group
    <get-igmp-group-information>
show igmp interface
    <get-igmp-interface-information>
show igmp output-group
    <get-igmp-output-group-information>
show igmp snooping
show igmp snooping interface
    <get-igmp-snooping-interface-information>
show igmp snooping interface bridge-domain
    <get-igmp-snooping-bridge-domain-interface>
show igmp snooping membership
    <get-igmp-snooping-membership-information>
show igmp snooping membership bridge-domain
show igmp snooping options
    <get-igmp-snooping-options-information>
show igmp snooping options
    get-igmp-snooping-options-information
show igmp snooping statistics
    <get-igmp-snooping-statistics-information>
show igmp snooping statistics bridge-domain
    <get-igmp-snooping-bridge-domain-membership>
show igmp statistics
    <get-igmp-statistics-information>

show ike
show ike security-associations
    <get-ike-security-associations-information>

show ilmi
    <get-ilmi-information>
```

```
show ilmi interface
<get-ilmi-interface-information>
show ilmi statistics
<get-ilmi-statistics>
show ingress-replication
  <get-ingress-replication-information>
show interfaces
  <get-interface-information>
show interfaces anchor-group
show interfaces controller
<get-interface-controller-information>
show interfaces destination-class
  <get-destination-class-statistics>

show interfaces destination-class all
<get-all-destination-class-statistics>
show interfaces diagnostics
show interfaces diagnostics optics
  <get-interface-optics-diagnostics-information>

show interfaces far-end-interval
  <show-interfaces-far-end-interval>
show interfaces filters
  <get-interface-filter-information>

show interfaces forwarding-class-counters
<get-interface-fc-counters-information>

show interfaces interface-set
<get-interface-set-information>
show interfaces interface-set queue
  <get-interface-set-queue-information>

show interfaces interval
  <show-interfaces-interval>
show interfaces load-balancing
  <interface-load-balancing>
show interfaces mac-database
  <get-mac-database>

show interfaces mc-ae
  <get-mc-ae-interface-information>
show interfaces mc-ae revertive-info
  <get-mc-ae-revertive-information>
show interfaces policers
  <get-interface-policer-information>

show interfaces queue
  <get-interface-queue-information>

show interfaces redundancy
  <get-redundancy-status>
show interfaces redundancy detail
  <get-redundancy-status-details>
show interfaces routing
show interfaces source-class
  <get-source-class-statistics>

show interfaces source-class all
<get-all-source-class-statistics>
show interfaces targeting
```

```
<get-targeting-information>
show interfaces transport
<get-interface-transport-information>
show interfaces transport optics
<get-interface-transport-optics-information>
show interfaces transport optics interval
<get-interface-transport-optics-interval-information>
show interfaces voq
<get-interface-voq-information>
show ipsec
show ipsec redundancy
show ipsec redundancy interface
  <get-ipsec-pic-redundancy-information>

show ipsec redundancy security-associations
  <get-ipsec-tunnel-redundancy-information>

show ipsec security-associations
  <get-security-associations-information>

show ipv6
show ipv6 neighbors
  <get-ipv6-nd-information>

show ipv6 router-advertisement
  <get-ipv6-ra-information>

show isis
show isis adjacency
  <get-isis-adjacency-information>

show isis authentication
  <get-isis-authentication-information>

show isis backup
show isis backup coverage
  <get-isis-backup-coverage-information>

show isis backup label-switched-path
  <get-isis-backup-lsp-information>

show isis backup spf

show isis backup spf results
  <get-isis-backup-spf-results-information>

show isis context-identifier
  <get-isis-context-identifier-information>

show isis context-identifier identifier
  <get-isis-context-identifier-origin-information>
show isis database
  <get-isis-database-information>

show isis hostname
  <get-isis-hostname-information>

show isis interface
  <get-isis-interface-information>

show isis overview
```

```
<get-isis-overview-information>

show isis route
  <get-isis-route-information>

show isis spf
show isis spf brief
  <get-isis-spf-results-brief-information>

show isis spf log
  <get-isis-spf-log-information>

show isis spf results
  <get-isis-spf-results-information>

show isis statistics
  <get-isis-statistics-information>

show l2-learning
show l2-learning backbone-instance
  <get-l2-learning-backbone-instance>
show l2-learning evpn
show l2-learning evpn arp-statistics
  <get-evpn-arp-statistics>
show l2-learning evpn arp-statistics interface
  <get-evpn-arp-statistics-interface>
show l2-learning global-information
  <get-l2-learning-global-information>
show l2-learning global-mac-count
  <get-l2-learning-global-mac-count>
show l2-learning instance
  <get-l2-learning-routing-instances>
show l2-learning interface
  <get-l2-learning-interface-information>
show l2-learning mac-move-buffer
  <get-l2-learning-mac-move-buffer-information>
show l2-learning provider-instance
  <get-l2-learning-provider-instance>
show l2-learning redundancy-groups
  <get-l2-learning-redundancy-groups>
show l2-learning remote-backbone-edge-bridges
  <get-l2-learning-remote-backbone-edge-bridges>
show l2-learning vxlan-tunnel-end-point
show l2-learning vxlan-tunnel-end-point remote
  <get-l2-learning-vxlan-rvtep-info>
show l2-learning vxlan-tunnel-end-point remote ip
  <get-l2-learning-vxlan-rvtep-ip-information>
show l2-learning vxlan-tunnel-end-point remote mac-table
  <get-l2-learning-vxlan-rvtep-mactable-information>
show l2-learning vxlan-tunnel-end-point remote vtep-source-interface
  <get-l2-learning-vxlan-remote-svtep-ip-information>
show l2-learning vxlan-tunnel-end-point source
  <get-l2-learning-vxlan-svtep-info>
show l2-learning vxlan-tunnel-end-point source ip
  <get-l2-learning-vxlan-svtep-ip-information>
show l2circuit
show l2circuit connections
  <get-l2ckt-connection-information>

show l2cpd
show l2cpd task
```



```
<get-l2cpd-task-information>
show l2cpd task io
  <get-l2cpd-tasks-io-statistics>
show l2cpd task memory
  <get-l2cpd-task-memory>
show l2cpd task replication
  <get-l2cpd-replication-information>
show l2vpn
show l2vpn connections
  <get-l2vpn-connection-information>

show lacp
show lacp interfaces
  <get-lacp-interface-information>
show lacp statistics
show lacp statistics interfaces
  <get-lacp-interface-statistics>
show lacp timeouts
show ldp
show ldp database
  <get-ldp-database-information>

show ldp fec-filters
  <get-ldp-fec-filters-information>

show ldp interface
  <get-ldp-interface-information>

show ldp neighbor
  <get-ldp-neighbor-information>

show ldp oam
  <get-ldp-oam-information>
show ldp overview
  <get-ldp-overview-information>
show ldp p2mp
show ldp p2mp fec
  <get-ldp-p2mp-fec-information>
show ldp p2mp path
  <get-ldp-p2mp-path-information>
show ldp p2mp tunnel
  <get-ldp-p2mp-tunnel-information>
show ldp path
  <get-ldp-path-information>

show ldp rib-groups
  <get-ldp-rib-groups-information>
show ldp route
  <get-ldp-route-information>

show ldp session
  <get-ldp-session-information>

show ldp statistics
  <get-ldp-statistics-information>

show ldp traffic-statistics
  <get-ldp-traffic-statistics-information>

show link-management
  <get-lm-information>
```

```
show link-management peer
  <get-lm-peer-information>

show link-management routing
  <get-lm-routing-information>

show link-management routing peer
  <get-lm-routing-peer-information>

show link-management routing resource
  <get-lm-routing-resource-information>

show link-management routing te-link
  <get-lm-routing-te-link-information>

show lldp
  <get-lldp-information>

show lldp detail
  <get-lldp-information-detail>

show lldp local-information
  <get-lldp-local-info>

show lldp neighbors
  <get-lldp-neighbors-information>

show lldp neighbors interface
  <get-lldp-interface-neighbors>
show lldp remote-global-statistics
  <get-lldp-remote-global-statistics>

show lldp statistics
  <get-lldp-statistics-information>

show lldp statistics interface
  <get-lldp-interface-statistics>
show link-management statistics
  <get-lm-statistics-information>

show link-management statistics peer
  <get-lm-peer-statistics>

show link-management te-link
  <get-lm-te-link-information>

show mac-rewrite
show mac-rewrite interface
  <get-mac-rewrite-interface-information>
show mld
show mld group
  <get-mld-group-information>

show mld interface
  <get-mld-interface-information>

show mld output-group
  <get-mld-output-group-information>

show mld snooping
```

```
show mld snooping interface
<get-mld-snooping-interface-information>
show mld snooping interface bridge-domain
<get-mld-snooping-bridge-domain-interface>
show mld snooping interface vlan
<get-mld-snooping-vlan-interface>
show mld snooping membership
<get-mld-snooping-membership-information>
show mld snooping membership bridge-domain
<get-mld-snooping-bridge-domain-membership>
show mld snooping membership vlan
<get-mld-snooping-vlan-membership>
show mld snooping statistics
<get-mld-snooping-statistics-information>
show mld snooping statistics bridge-domain
<get-mld-snooping-bridge-domain-statistics>
show mld snooping statistics vlan
<get-mld-snooping-vlan-statistics>
show mld statistics
<get-mld-statistics-information>

show mobile-ip
show mobile-ip home-agent
show mobile-ip home-agent binding
<get-mip-binding-information>

show mobile-ip home-agent binding ip-address
<get-ip-mip-binding-information>

show mobile-ip home-agent binding nai
<get-nai-mip-binding-information>

show mobile-ip home-agent binding summary
<get-summary-mip-binding-information>

show mobile-ip home-agent interface
<get-mip-ha-interface-information>

show mobile-ip home-agent overview
<get-mip-ha-overview-information>

show mobile-ip home-agent traffic
<get-mip-ha-traffic-information>

show mobile-ip home-agent virtual-network
<get-mip-ha-virtual-network-information>

show mobile-ip tunnel
<get-mip-tunnel-information>
show mobile-ip wimax
show mobile-ip wimax release
<get-mip-wimax-release-information>

show mpls
show mpls admin-groups
<get-mpls-admin-group-information>

show mpls admin-groups-extended
<get-mpls-admin-group-extended-information>
show mpls call-admission-control
<get-mpls-call-admission-control-information>
```

```
show mpls context-identifier
    <get-mpls-context-identifier-information>

show network-access domain-map
show network-access domain-map statistics
    <get-domain-map-statistics>
show mpls cspf
    <get-mpls-cspf-information>

show mpls diffserv-te
    <get-mpls-diffserv-te-information>
show mpls egress-protection
show mpls interface
    <get-mpls-interface-information>
show mpls label
    <get mpls-label-space>
show mpls label usage
    <get mpls-label-space-usage>

show mpls lsp
    <get-mpls-lsp-information>

show mpls lsp autobandwidth
    <get-mpls-lsp-autobandwidth>
show mpls srlg
    <get-mpls-srlg-information>
show oam ethernet fnp
show oam ethernet fnp interface
show oam ethernet fnp messages
show oam ethernet fnp status
    <get-fnp-status>
show mpls lsp defaults
    <get-mpls-lsp-defaults-information>

show mpls path
    <get-mpls-path-information>

show mpls static-lsp
    <get-mpls-static-lsp-information>
show mpls traceroute
show mpls traceroute database
show mpls traceroute database ldp
    <get-mpls-traceroute-database-ldp>
show msdp
    <get-msdp-information>
show msdp source
    <get-msdp-source-information>

show msdp source-active
    <get-msdp-source-active-information>

show msdp statistics
    <get-msdp-statistics-information>

show multicast
show multicast backup-pe-groups
    <get-multicast-backup-pe-groups-information>

show multicast backup-pe-groups address
    <get-multicast-backup-pe-address-information>
```

```
show multicast backup-pe-groups group
<get-multicast-backup-pe-group-information>
show multicast flow-map
<get-multicast-flow-maps-information>

show multicast interface
<get-multicast-interface-information>

show multicast next-hops
<get-multicast-next-hops-information>

show multicast pim-to-igmp-proxy
<get-multicast-pim-to-igmp-proxy-information>

show multicast pim-to-mld-proxy
<get-multicast-pim-to-mld-proxy-information>

show multicast route
<get-multicast-route-information>

show multicast rpf
<get-multicast-rpf-information>

show multicast scope
<get-multicast-scope-information>

show multicast sessions
<get-multicast-sessions-information>

show multicast snooping
show multicast snooping next-hops
<get-multicast-snooping-next-hops-information>

show multicast snooping route
<get-multicast-snooping-route-information>

show multicast statistics
<get-multicast-statistics-information>

show multicast usage
<get-multicast-usage-information>

show mvpn
show mvpn c-multicast
<get-mvpn-c-multicast-information>
show mvpn instance
<get-mvpn-instance-information>

show mvpn neighbor
<get-mvpn-neighbor-information>
show mvrp
<get-mvrp-information>

show mvrp applicant-state
<get-mvrp-applicant-information>

show mvrp dynamic-vlan-memberships
<get-mvrp-dynamic-vlan-memberships>

show mvrp interface
```

```
<get-mvrp-interface-information>

show mvrp registration-state
  <get-mvrp-registration-state>

show mvrp statistics
  <get-mvrp-interface-statistics>

show network-access
show network-access aaa
show network-access aaa radius-servers
  <get-radius-servers-table>
show network-access aaa statistics
  <get-aaa-module-statistics>

show network-access aaa statistics address-assignment
show network-access aaa statistics address-assignment client
  <get-address-assignment-client-statistics>
show network-access aaa statistics address-assignment pool
  <get-address-assignment-pool-statistics>
show network-access aaa subscribers
  <get-aaa-subscriber-table>

show network-access aaa subscribers session-id

show network-access aaa subscribers statistics
  <get-aaa-subscriber-statistics>

show network-access aaa terminate-code
  <get-aaa-terminate-code>
show network-access aaa terminate-code aaa
  <get-aaa-terminate-code-aaa>
show network-access aaa terminate-code dhcp
  <get-aaa-terminate-code-dhcp>
show network-access aaa terminate-code l2tp
  <get-aaa-terminate-code-l2tp>
show network-access aaa terminate-code ppp
  <get-aaa-terminate-code-ppp>
show network-access aaa terminate-code reverse
  <get-aaa-terminate-code-reverse>
show network-access aaa terminate-code reverse aaa
  <get-aaa-terminate-code-reverse-aaa>
show network-access aaa terminate-code reverse dhcp
  <get-aaa-terminate-code-reverse-dhcp>
show network-access aaa terminate-code reverse l2tp
  <get-aaa-terminate-code-reverse-l2tp>
show network-access aaa terminate-code reverse ppp
  <get-aaa-terminate-code-reverse-ppp>
show network-access address-assignment
show network-access address-assignment pool
  <get-address-assignment-pool-table>

show network-access requests
show network-access requests pending
  <get-authentication-pending-table>

show network-access requests statistics
  <get-authentication-statistics>

show network-access securid-node-secret-file
  <get-node-secret-file-table>
```

```
show nonstop-routing
<get-nonstop-routing-information>

show ntp
show ntp associations
show ntp status
show oam
show oam ethernet
show oam ethernet connectivity-fault-management
show oam ethernet connectivity-fault-management adjacencies
<get-cfm-adjacency-information>
show oam ethernet connectivity-fault-management delay-statistics
<get-cfm-delay-statistics>

show oam ethernet connectivity-fault-management forwarding-state
show oam ethernet connectivity-fault-management forwarding-state instance
<get-cfm-forwarding-state-instance-information>

show oam ethernet connectivity-fault-management forwarding-state interface
<get-cfm-forwarding-state-interface-information>

show oam ethernet connectivity-fault-management interfaces
<get-cfm-interfaces-information>
show oam ethernet connectivity-fault-management loss-statistics
<get-cfm-loss-statistics>
show oam ethernet connectivity-fault-management mep-database
<get-cfm-mep-database>

show oam ethernet connectivity-fault-management mep-statistics
<get-cfm-mep-statistics>

show oam ethernet connectivity-fault-management mip
<get-cfm-mip-information>

show oam ethernet connectivity-fault-management path-database
<get-cfm-linktrace-path-database>

show oam ethernet connectivity-fault-management policer
<get-evc-information>

show oam ethernet connectivity-fault-management sla-iterator-statistics
<get-cfm-iterator-statistics>
show oam ethernet evc
<get-evc-information>
show oam ethernet link-fault-management
<get-lfmd-information>

show oam ethernet lmi
<get-elmi-information>

show oam ethernet lmi statistics
<get-elmi-statistics>

show openflow
show openflow capability
show openflow controller
show openflow filters
show openflow flows
show openflow interfaces
show openflow statistics
```

```
show openflow statistics flows
show openflow statistics interfaces
show openflow statistics packet
show openflow statistics packet in
show openflow statistics packet out
show openflow statistics queue
show openflow statistics summary
show openflow statistics tables
show openflow summary
show openflow switch

show ospf
show ospf backup
show ospf backup coverage
    <get-ospf-backup-coverage-information>

show ospf backup lsp
    <get-ospf-backup-lsp-information>

show ospf backup neighbor
    <get-ospf-backup-neighbor-information>

show ospf backup spf
    <get-ospf-backup-spf-information>

show ospf context-identifier
    <get-ospf-context-id-information>

show ospf database
    <get-ospf-database-information>

show ospf interface
    <get-ospf-interface-information>

show ospf io-statistics
    <get-ospf-io-statistics-information>

show ospf log
    <get-ospf-log-information>

show ospf neighbor
    <get-ospf-neighbor-information>

show ospf overview
    <get-ospf-overview-information>

show ospf route
    <get-ospf-route-information>

show ospf statistics
    <get-ospf-statistics-information>

show ospf3
show ospf3 backup
show ospf3 backup coverage
    <get-ospf3-backup-coverage-information>

show ospf3 backup lsp
    <get-ospf3-backup-lsp-information>

show ospf3 backup neighbor
```



```
<get-ospf3-backup-neighbor-information>

show ospf3 backup spf
<get-ospf3-backup-spf-information>

show ospf3 database
<get-ospf3-database-information>

show ospf3 interface
<get-ospf3-interface-information>

show ospf3 io-statistics
<get-ospf3-io-statistics-information>

show ospf3 log
<get-ospf3-log-information>

show ospf3 neighbor
<get-ospf3-neighbor-information>

show ospf3 overview
<get-ospf3-overview-information>

show ospf3 route
<get-ospf3-route-information>

show ospf3 statistics
<get-ospf3-statistics-information>

show passive-monitoring
<get-passive-monitoring-information>

show passive-monitoring error
<get-passive-monitoring-error-information>

show passive-monitoring flow
<get-passive-monitoring-flow-information>

show passive-monitoring memory
<get-passive-monitoring-memory-information>

show passive-monitoring status
<get-passive-monitoring-status-information>

show passive-monitoring usage
<get-passive-monitoring-usage-information>
show path-computation-client
show path-computation-client active-pce
show path-computation-client statistics
show performance-monitoring
show performance-monitoring mpls
show performance-monitoring mpls lsp
<get-pm-mpls-lsp-information>
show pfe
show pfe cfeb
show pfe feb
show pfe filter
show pfe filter hw
show pfe filter hw summary
show pfe fpc
show pfe fwdd
```

```
show pfe lcc
show pfe next-hop
show pfe pfem
show pfe pfem detail
show pfe pfem extensive
show pfe route
show pfe route clnp
show pfe route clnp table
show pfe route inet6
show pfe route inet6 hw
show pfe route inet6 hw host
show pfe route inet6 hw lpm
show pfe route inet6 hw multicast

show pfe route inet6 table
show pfe route ip
show pfe route ip table
show pfe route iso
show pfe route iso table
show pfe scb
show pfe sfm
show pfe ssb
show pfe statistics
show pfe statistics exceptions
show pfe statistics fabric
show pfe statistics ip
show pfe route ip hw
show pfe route ip hw host
show pfe route ip hw lpm
show pfe route ip hw multicast
show pfe route summary
show pfe route summary hw
show pfe statistics ip6
show pfe statistics traffic
    <get-pfe-statistics>

show pfe statistics traffic cpu
show pfe statistics traffic cpu fpe
show pfe statistics traffic detail
<get-pfe-traffic-statistics>
show pfe statistics traffic egress-queues
show pfe statistics traffic egress-queues fpc
show pfe statistics traffic multicast
show pfe statistics traffic multicast fpcshow pfe statistics traffic protocol
show pfe terse
    <get-pfe-information>

show pfe version brief
show pfe version detail
show pgm
show pgm negative-acknowledgments
    <get-pgm-nak>

show pgm source-path-messages
    <get-pgm-source-path-messages>

show pgm statistics
    <get-pgm-statistics>

show pim
show pim bidirectional
```

```
show pim bidirectional df-election
<get-pim-bidir-df-election-information>
show pim bidirectional df-election interface
<get-pim-bidir-df-election-interface-information>
show pim bootstrap
<get-pim-bootstrap-information>

show pim interfaces
<get-pim-interfaces-information>

show pim join
<get-pim-join-information>

show pim mdt
<get-pim-mdt-information>

show pim mdt data-mdt-joins
<get-pim-data-mdt-join-information>
show pim mvpn
<get-pim-mvpn-information>

show pim neighbors
<get-pim-neighbors-information>

show pim rps
<get-pim-rps-information>
show pim snooping
show pim snooping interfaces
show pim snooping join
show pim snooping neighbors
show pim snooping statistics
show pim source
<get-pim-source-information>

show pim statistics
<get-pim-statistics-information>

show policy
show policy conditions
show policy damping
show ppp
show ppp address-pool
<get-ppp-address-pool-information>

show ppp interface
<get-ppp-interface-information>

show ppp statistics
<get-ppp-statistics-information>

show ppp summary
<get-ppp-summary-information>

show pppoe
show pppoe interfaces
<get-pppoe-interface-information>
show pppoe lockout
<get-pppoe-lockout-information>

show pppoe service-name-tables
<get-pppoe-service-name-table-information>
```

```
show pppoe statistics
    <get-pppoe-statistics-information>

show pppoe underlying-interfaces
    <get-pppoe-underlying-interface-information>

show pppoe version
    <get-pppoe-version>

show protection-group
show protection-group ethernet-aps
    <show-protection-group-ethernet-aps>
show protection-group ethernet-ring
show protection-group ethernet-ring aps
    <get-raps-pdu-information>
show protection-group ethernet-ring data-channel
    <get-ring-data-channel-information>
show protection-group ethernet-ring interface
    <get-ring-interface-information>
show protection-group ethernet-ring node-state
    <get-raps-state-machine-information>
show protection-group ethernet-ring node-state
show protection-group ethernet-ring statistics
    <get-ring-tatistics>
show protection-group ethernet-ring vlan
    <get-ring-vlan-information>

show ptp
show ptp clock
    get-ntp-clock>
show ptp global-information
    get-ntp-global-information>
show ptp hybrid
show ptp hybrid config
    <get-ntp-hybrid-mapping>
show ptp hybrid status
    <get-ntp-hybrid-status>
show ptp last-tod-update
    <get-last-tod-update>
show ptp lock-status
    get-ntp-lock-status>
show ptp master
    <get-ntp-master>
show ptp path-trace
    <get-ntp-path-trace>
show ptp port
    <get-ntp-port>
show ptp quality-level-mapping
    <get-ntp-quality-level-mapping>
show ptp slave
    <get-ntp-slave>
show ptp stateful
    <get-ntp-stateful>
show ptp statistics
    <get-ntp-statistics>
show r2cp
show r2cp interfaces
    <get-r2cp-interface-information>
show r2cp radio
    <get-r2cp-radio-information>
show r2cp sessions
```

```
<get-r2cp-session-information>
show r2cp statistics
  <get-r2cp-statistics>
show redundant-power-system
show redundant-power-system led
show redundant-power-system multi-backup
<get-rps-scale-information>
show redundant-power-system network
<get-rps-network-information>
show redundant-power-system power-supply
show redundant-power-system status
show redundant-power-system upgrade
<get-rps-upgrade-information>
show redundant-power-system version
show rip
show rip general-statistics
  <get-rip-general-statistics-information>

show rip neighbor
  <get-rip-neighbor-information>

show rip statistics
  <get-rip-statistics-information>
show rip statistics peer
  <get-rip-peer-information>
show ripng
show ripng general-statistics
  <get-ripng-general-statistics-information>

show ripng neighbor
  <get-ripng-neighbor-information>
show ripng statistics
  <get-ripng-statistics-information>
show route
  <get-route-information>

show route cumulative
  <get-route-cumulative>

show route export
  <get-rtexport-table-information>

show route export instance
  <get-rtexport-instance-information>

show route localization
  <get-fib-localization-information>
show route export vrf-target
  <get-rtexport-target-information>

show route flow
show route flow validation
  <get-rtflow-dep-information>

show route forwarding-table
  <get-forwarding-table-information>

show route instance
  <get-instance-information>

show route instance operational
```

```
<get-operational-routing-instance-information>

show route martians
<get-route-martians>
show route resolution
<get-route-resolution-information>
show route resolution summary
<get-route-resolution-summary>
show route resolution unresolved
show route rib-groups
<get-route-rib-groups>
show route snooping
<get-route-snooping-information>
show route snooping summary
<get-route-snooping-summary>
show route summary
<get-route-summary-information>

show rsvp
show rsvp interface
<get-rsvp-interface-information>

show rsvp neighbor
<get-rsvp-neighbor-information>

show rsvp session
<get-rsvp-session-information>

show rsvp statistics
<get-rsvp-statistics-information>

show rsvp version
<get-rsvp-version-information>

show sap
show sap listen
<get-sap-listen-information>
show security group-vpn member kek
show security group-vpn member kek security-associations
<get-gvpn-kek-security-associations-information>

show services
show services accounting
<get-service-accounting-information>

show services accounting aggregation
<get-service-accounting-aggregation-information>

show services accounting aggregation as
<get-service-accounting-aggregation-as-information>

show services accounting aggregation destination-prefix
<get-service-accounting-aggregation-destination-prefix-information>

show services accounting aggregation protocol-port
<get-service-accounting-aggregation-protocol-port-information>

show services accounting aggregation source-destination-prefix
<get-service-accounting-aggregation-source-destination-prefix-information>

show services accounting aggregation source-prefix
```

```

    <get-service-accounting-aggregation-source-prefix-information>

show services accounting aggregation template
    <get-service-accounting-aggregation-template-information>

show services accounting errors
    <get-service-accounting-errors-information>

show services accounting flow
    <get-service-accounting-flow-information>

show services accounting flow-detail
    <get-service-accounting-flow-detail>

show services accounting memory
    <get-service-accounting-memory-information>

show services accounting packet-size-distribution
    <get-packet-distribution-information>

show services accounting status
    <get-service-accounting-status-information>

show services accounting usage
    <get-service-accounting-usage-information>

show services alg
show services alg conversations
    <get-service-msp-alg-conversation-information>
show services alg sip-globals
    <get-service-msp-alg-sip-globals-information>
show services alg statistics
show services application-aware-access-list
show services application-aware-access-list flows
show services application-aware-access-list flows interface
    <get-application-aware-access-list-flows-interface>
show services application-aware-access-list flows subscriber
    <get-application-aware-access-list-flows-subscriber>
show services application-aware-access-list statistics
show services application-aware-access-list statistics interface
    <get-application-aware-access-list-statistics-interface>
show services application-aware-access-list statistics subscriber
    <get-application-aware-access-list-statistics-subscriber>
show services application-identification
show services application-identification application
show services application-identification application detail
    <get-appid-application-signature-detail>
show services application-identification application summary
    <get-appid-application-signature-summary>
show services application-identification application-system-cache
    <get-appid-application-system-cache>

show services application-identification counter
    <get-appid-counter>
show services application-identification counter ssl-encrypted-sessions
    <get-appid-counter-encrypted>
show services application-identification group
show services application-identification group detail

    <get-appid-application-group-detail>
show services application-identification group summary

```

```
<get-appid-application-group-summary>
show services application-identification statistics
show services application-identification statistics application-groups
<get-appid-application-group-statistics>
show services application-identification statistics applications
<get-appid-application-statistics>
show services application-identification version
<get-appid-package-version>

show services border-signaling-gateway
show services border-signaling-gateway accounting
show services border-signaling-gateway accounting statistics
<get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway accounting status
<get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway admission-control
<get-service-border-signaling-gateway-statistics-admission-control>

show services border-signaling-gateway by-call-context-id
<get-service-bsg-information-by-call-context-id>

show services border-signaling-gateway by-contact
<get-service-border-signaling-gateway-information-by-contact>

show services border-signaling-gateway by-request-uri
<get-service-border-signaling-gateway-information-by-request-uri>

show services border-signaling-gateway calls
<get-service-border-signaling-gateway-statistics-calls>

show services border-signaling-gateway calls-duration
<get-service-border-signaling-gateway-calls-duration>

show services border-signaling-gateway calls-failed

how services border-signaling-gateway charging
show services border-signaling-gateway charging statistics
<get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway charging status
<get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway denied-messages
<get-service-bsg-denied-messages>

show services border-signaling-gateway embedded-spdf
<get-service-border-signaling-gateway-embedded-spdf>

show services border-signaling-gateway embedded-spdf status
<get-service-border-signaling-gateway-embedded-spdf-status>

show services border-signaling-gateway name-resolution-cache

show services border-signaling-gateway name-resolution-cache all
<get-service-border-signaling-gateway-name-resolution-cache-all>

show services border-signaling-gateway name-resolution-cache by-fqdn
<get-border-signaling-gateway-name-resolution-cache-by-fqdn>
show services border-signaling-gateway status
<get-service-bsg-status-information>
show services captive-portal-content-delivery
show services captive-portal-content-delivery pic
```



```
<get-cpcd-pic-information>
show services captive-portal-content-delivery profile
<get-cpcd-profile>
show services captive-portal-content-delivery rule
<get-cpcd-rule>
show services captive-portal-content-delivery ruleset
<get-cpcd-rule-set>
show services captive-portal-content-delivery sset
<get-cpcd-service-set>
show services captive-portal-content-delivery statistics
<get-cpcd-pic-statistics>
show services captive-portal-content-delivery statistics interface
show services capture
<get-service-capture>
show services cos
show services cos statistics
<get-service-cos-statistics-information>

show services cos statistics diffserv
<get-service-cos-diffserv-statistics>

show services cos statistics forwarding-class
<get-service-cos-forwarding-class-statistics>

show services crtp
<get-service-crtp-params-information>

show services crtp extensive
<get-service-crtp-extensive-information>

show services crtp flows
<get-service-crtp-flow-table-information>

show services dynamic-flow-capture
show services dynamic-flow-capture content-destination
<get-services-dynamic-flow-capture-content-destination-information>

show services dynamic-flow-capture control-source
<get-services-dynamic-flow-capture-control-source-information>

show services dynamic-flow-capture statistics
<get-services-dfc-statistics-information>
show services fips
show services fips pic
show services fips pic status
<get-fips-pic-status-information>

show services flow-collector
<get-services-flow-collector-information>

show services flow-collector file
<get-services-flow-collector-file-information>

show services flow-collector input
<get-services-flow-collector-input-information>

show services flow-table
show services flow-table statistics
<get-flow-table-statistics-information>

show services flows
```

```
<get-service-msp-flow-table-information>

show services ggsn
show services ggsn diagnostics
show services ggsn diagnostics pdp
    <get-pdp-diagnostics-per-apn>

show services ggsn statistics
    <get-ggsn-statistics>

show services ggsn statistics apn
    <get-ggsn-apn-statistics-information>

show services ggsn statistics charging
    <get-ggsn-charging-statistics-information>

show services ggsn statistics gtp
    <get-ggsn-gtp-statistics-information>

show services ggsn statistics gtp-prime
    <get-ggsn-gtp-prime-statistics-information>

show services ggsn statistics imsi
    <get-ggsn-imsi-user-information>

show services ggsn statistics l2tp-tunnel
    <get-ggsn-l2tp-tunnel-statistics-information>

show services ggsn statistics msisdn
show services ggsn statistics radius
    <get-ggsn-radius-statistics-information>

show services ggsn statistics sgsn
    <get-ggsn-sgsn-statistics-information>

show services ggsn status
    <get-ggsn-interface-information>

show services ggsn trace
show services ggsn trace all
    <get-ggsn-trace>

show services ggsn trace imsi
    <get-ggsn-imsi-trace>

show services ggsn trace msisdn
    <get-ggsn-msisdn-trace>
show services hcm
show services hcm pic-statistics
    <get-service-hcm-pic-statistics-information>
show services ids
show services ids destination-table
    <get-service-ids-destination-table-information>

show services ids pair-table
    <get-service-ids-pair-table-information>

show services ids source-table
    <get-service-ids-source-table-information>

show services inline
```

```
show services inline ip-reassembly
show services inline ip-reassembly statistics
show services inline nat
show services inline nat mappings
show services inline nat mappings nptv6
<get-inline-nat-mapping-nptv6-information>
show services inline nat pool
  <get-inline-nat-pool-information>
show services inline nat statistics
  <get-inline-nat-statistics-information>
show services inline software
show services inline software statistics
<get-inline-service-sw-statistics-information>
show services inline stateful-firewall
show services inline stateful-firewall flows
<get-inline-sfw-flow-table-information>
show services inline stateful-firewall statistics
<get-inline-sfw-statistics-information>
show services ipsec-vpn
show services ipsec-vpn ike
show services ipsec-vpn ike security-associations
  <get-ike-services-security-associations-information>

show services ipsec-vpn ike statistics
<get-ike-services-statistics>
show services ipsec-vpn ipsec
show services ipsec-vpn ipsec security-associations
  <get-services-security-associations-information>

show services ipsec-vpn ipsec statistics
  <get-services-ipsec-statistics-information>

show services l2tp
show services l2tp destination
  <get-l2tp-destination-information>
show services l2tp destination lockout
<get-services-l2tp-destination-lockout>
show services l2tp disconnect-cause-summary<
<get-l2tp-disconnect-cause-summary>
show services l2tp multilink
  <get-l2tp-multilink-information>

show services l2tp radius
show services l2tp radius accounting
show services l2tp radius accounting servers
  <get-services-l2tp-radius-accounting-servers-information>

show services l2tp radius accounting statistics
  <get-services-l2tp-radius-accounting-statistics-information>

show services l2tp radius authentication
show services l2tp radius authentication servers
  <get-services-l2tp-radius-authentication-servers-information>

show services l2tp radius authentication statistics
  <get-services-l2tp-radius-authentication-statistics-information>

show services l2tp radius servers
  <get-services-l2tp-radius-authentication-accounting-servers-information>

show services l2tp radius statistics
```

```
<get-services-l2tp-radius-authentication-accounting-statistics-information>

show services l2tp session
  <get-l2tp-session-information>

show services l2tp summary
  <get-l2tp-summary-information>

show services l2tp tunnel
  <get-l2tp-tunnel-information>

show services l2tp user
  <get-l2tp-user-information>
show services link-services
show services link-services cpu-usage
  <get-link-services-cpu-usage>

show services local-policy-decision-function
show services local-policy-decision-function flows
show services local-policy-decision-function flows interface
  <get-local-policy-decision-function-flows-interface>
show services local-policy-decision-function flows subscriber
  <get-local-policy-decision-function-flows-subscriber>
show services local-policy-decision-function statistics
show services local-policy-decision-function statistics interface
  <get-local-policy-decision-function-statistics-interface>
show services local-policy-decision-function statistics subscriber
  <get-local-policy-decision-function-statistics-subscriber>
show services logging
show services logging history
show services logging history client
show services logging logfiles
show services mobile
show services mobile hcm
show services mobile hcm statistics
show services nat
show services nat ipv6-multicast-interfaces
  <get-service-nat-ipv6-multicast-information>

show services nat deterministic-nat
show services nat deterministic-nat internal-host
show services nat deterministic-nat nat-port-block
show services nat mappings
  <get-service-nat-mapping-address-pooling-paired>
show services nat mappings brief
  <get-service-nat-mapping-brief>
show services nat mappings detail
  <get-service-nat-mapping-endpoint-independent>
show services nat mappings brief
  <get-service-nat-mapping-brief>
show services nat mappings detail
  <get-service-nat-mapping-detail>
show services nat mappings pcp
show services nat mappings summary
  <get-service-nat-mapping-summary>
show services nat pool
  <get-service-nat-pool-information>
show services pcp
show services pgcp
show services pgcp active-configuration
```

```
<get-pgcpd-active-configuration>

show services pgcp active-configuration gateway
<get-service-pgcp-active-configuration-gateway>

show services pgcp conversations
<get-service-pgcp-conversation-information>

show services pgcp conversations gateway
<get-service-pgcp-conversation-information-gateway>

show services pgcp flows
<get-service-pgcp-flow-table-information>

show services pgcp flows gateway
<get-service-pgcp-flow-table-information-gateway>

show services pgcp gate
<get-service-pgcp-gate>

show services pgcp gate gateway
<get-service-pgcp-gate-gateway>

show services pgcp gates
<get-service-pgcp-gates>

show services pgcp gates gateway
<get-service-pgcp-gates-gateway>

show services pgcp root-termination
<get-services-pgcpd-root-termination>

show services pgcp root-termination gateway
<get-services-pgcpd-root-termination-gateway>

show services pgcp statistics
<get-service-pgcp-statistics>

show services pgcp statistics gateway
<get-service-pgcp-statistics-gateway>

show services pgcp terminations
<get-service-pgcp-terminations>

show services pgcp terminations gateway
<get-service-pgcp-terminations-gateway>

show services rpm
show services rpm active-servers
<get-active-servers>

show services rpm history-results
<get-history-results>

show services rpm probe-results
<get-probe-results>

show services rpm twamp
<twamp-information>
show services rpm twamp client
<twamp-client-information>
```

```
show services rpm twamp client connection
<twamp-client-connection-information>
show services rpm twamp client history-results
<twamp-get-history-results>
show services rpm twamp client probe-results
<twamp-get-probe-results>
show services rpm twamp client session
<twamp-client-test-session>
show services rpm twamp server
<twamp-server-information>
show services rpm twamp server connection
<twamp-server-connection-information>
show services rpm twamp server session
<twamp-server-session-information>
show services server-load-balance
show services server-load-balance external-manager
show services server-load-balance external-manager information
show services server-load-balance external-manager statistics
<get-external-manager-statistics-information>
show services server-load-balance hash-table
<get-hash-table-information>
show services server-load-balance health-monitor
show services server-load-balance health-monitor information
<get-real-server-health-monitor-information>
show services server-load-balance health-monitor statistics
<get-real-server-health-monitor-statistics-information>
show services server-load-balance real-server
show services server-load-balance real-server statistics
<get-real-server-statistics-information>
show services server-load-balance real-server-group
show services server-load-balance real-server-group information
<get-real-server-group-information>
show services server-load-balance real-server-group statistics
<get-real-server-group-statistics-information>
show services server-load-balance sticky
<get-sticky-table-information>
show services server-load-balance virtual-server
show services server-load-balance virtual-server information
<get-virtual-server-information>
show services server-load-balance virtual-server statistics
<get-virtual-server-statistics-information>
show services service-identification
show services service-identification header-redirect
show services service-identification header-redirect statistics
<get-header-redirect-set-statistics-information>

show services service-identification statistics
<get-service-identification-statistics-information>

show services service-identification uri-redirect
show services service-identification uri-redirect statistics
<get-uri-redirect-set-statistics-information>

show services service-sets
show services service-sets cpu-usage
<get-service-set-cpu-statistics>

show services service-sets memory-usage
<get-service-set-memory-statistics>

show services service-sets memory-usage zone
```

```
show services service-sets plug-ins
  <get-service-set-plugin-summary>

show services service-sets statistics
show services service-sets statistics drop-flow-limit
  <get-service-set-drop-flow-statistics>
show services service-sets statistics jflow-log
  <get-service-set-jflow-log-statistics>
show services service-sets statistics packet-drops
  <get-service-set-packet-drop-statistics>

show services service-sets statistics syslog
  <get-service-set-syslog-statistics>
show services service-sets statistics tcp-mss
  <get-service-set-tcp-mss-statistics>

show services service-sets summary
  <get-service-set-summary-information>

show services sessions
  <get-msp-session-table>

show services software
  <get-service-software-table-information>

show services software flows
  <get-service-fwnat-flow-table-information>

show services software statistics
  <get-service-software-statistics-information>

show services stateful-firewall
show services stateful-firewall flow-analysis
  <get-service-flow-analysis-information>
show services stateful-firewall conversations
  <get-service-sfw-conversation-information>

show services stateful-firewall flows
  <get-service-sfw-flow-table-information>
show services stateful-firewall redundancy-statistics
  <get-service-sfw-redundancy-statistics>

show services stateful-firewall sip-call
  <get-service-sfw-sip-call-information>

show services stateful-firewall sip-register
  <get-service-sfw-sip-register-information>

show services stateful-firewall statistics
  <get-service-sfw-statistics-information>

show services stateful-firewall statistics application-protocol
  <et-sfw-application-protocol-statistics>
show services stateful-firewall subscriber-analysis
  <get-service-subs-analysis-information>
show services subscriber
show services subscriber bandwidth
show services subscriber bandwidth client-id
  <get-services-subscriber-bandwidth-by-session-id>
show services subscriber bandwidth interface
```

```
<get-services-subscriber-bandwidth-by-interface>
show services subscriber bandwidth ip-address
<get-services-subscriber-bandwidth-by-ip-address>
show services subscriber bandwidth service-interface
<get-services-subscriber-bandwidth-by-service-interface>
show services subscriber dynamic-policies
<get-services-subscriber-dynamic-policies>
show services subscriber flows
<get-services-subscriber-flows>
show services subscriber sessions
<get-services-subscriber-session>
show services subscriber statistics
<get-services-subscriber-statistics>
show services unified-access-control
show services unified-access-control authentication-table
<get-uac-auth-table>
show services unified-access-control policies
<get-uac-policies>
show services unified-access-control roles
<get-uac-role-entries>
show services unified-access-control status
<get-uac-status>
show services video-monitoring
<get-service-video-monitoring-information>
show services video-monitoring mdi
<get-service-video-monitoring-mdi-information>
show services video-monitoring mdi alarms
<get-services-video-monitoring-mdi-alarms-information>
show services video-monitoring mdi alarms errors
<get-services-video-monitoring-mdi-alarms-errors-information>
show services video-monitoring mdi alarms stats
<get-services-video-monitoring-mdi-alarms-stats-information>
show services video-monitoring mdi errors
<get-service-video-monitoring-mdi-errors-information>
show services video-monitoring mdi flow
<get-service-video-monitoring-mdi-flows-information>
show services video-monitoring mdi stats
<get-service-video-monitoring-mdi-stats-information>
show snmp
show snmp health-monitor
<get-health-monitor-information>

show snmp health-monitor alarms
<get-health-monitor-alarm-information>

show snmp health-monitor logs
<get-health-monitor-log-information>

show snmp inform-statistics
<get-snmp-inform-statistics>

show snmp mib
show snmp mib get
<get-snmp-object>

show snmp mib get-next
<get-next-snmp-object>

show snmp mib walk
<get-walk-snmp-object>
```



```
show snmp proxy
show snmp rmon
    <get-rmon-information>

show snmp rmon alarms
    <get-rmon-alarm-information>

show snmp rmon events
    <get-rmon-event-information>

show snmp rmon history
    <get-rmon-history-information>

show snmp rmon logs
    <get-rmon-log-information>

show snmp statistics
    <get-snmp-information>

show snmp v3
    <get-snmp-v3-information>

show snmp v3 access
    <get-snmp-v3-access-information>

show snmp v3 community
    <get-snmp-v3-community-information>

show snmp v3 general
    <get-snmp-v3-general-information>

show snmp v3 groups
    <get-snmp-v3-group-information>

show snmp v3 notify
    <get-snmp-v3-notify-information>

show snmp v3 notify filter
    <get-snmp-v3-notify-filter-information>

show snmp v3 target
    <get-snmp-v3-target-information>

show snmp v3 target address
    <get-snmp-v3-target-address-information>

show snmp v3 target parameters
    <get-snmp-v3-target-parameters-information>

show snmp v3 users
    <get-snmp-v3-usm-user-information>

show spanning-tree
show spanning-tree bridge
    <get-stp-bridge-information>
show spanning-tree interface
    <get-stp-interface-information>
show spanning-tree mstp
show spanning-tree mstp configuration
    <get-mstp-configuration-information>
show spanning-tree statistics
```

```
<get-stp-interface-statistics>
show spanning-tree statistics bridge
show spanning-tree statistics interface
show spanning-tree statistics routing-instance
<get-stp-routing-instance-statistics>
show spanning-tree stp-buffer
show static-subscribers
show static-subscribers sessions
<show subscribers
  <get-subscribers>
show subscribers summary
  <get-subscribers-summary>
<get-syslog-filenames>

show synchronous-ethernet
show synchronous-ethernet esmc
show synchronous-ethernet esmc statistics
show synchronous-ethernet esmc transmit
show synchronous-ethernet global-information
show system
show system alarms
  <get-system-alarm-information>

show system auto-snapshot
show system boot-messages
show system buffers
show system certificate
show system commit
  <get-commit-information>
show system commit revision
  <get-commit-revision-information>
show system commit server
  <get-commit-server-information>
show system commit server queue
  <get-commit-server-queue-information>
show system configuration
show system configuration archival
  <get-system-archival>

show system configuration rescue
  <get-rescue-information>

show system connections
show system core-dumps
  <get-system-core-dumps>
show system core-dumps core-file-info
  <get-core-file-information>

show system core-dumps kernel-crashinfo
show system core-dumps transfer-status
show system diagnostics
show system diagnostics inventory
show system diagnostics usage
show system directory-usage
  <get-directory-usage-information>

show system firmware
  <get-system-firmware-information>
show system khms-stats
```

```
show system license
  <get-license-summary-information>

show system license installed
  <get-license-information>
show system license key-content
show system license keys
  <get-license-key-information>

show system license usage
  <get-license-usage-summary>
show system login
show system login lockout
  <get-system-login-lockout-information>
show system memory
<show system processes
show system processes brief
show system processes esc-node
show system processes extensive
show system processes health
  <get-process-health-information>

show system processes providers
show system processes host-processes detail
show system processes resource-limits
  <get-system-process-resource-limits>
show system processes summary
show system queues
show system reboot
show system resource-cleanup
show system resource-cleanup processes
  <get-system-resource-cleanup-processes-information>
  <get-resource-monitor-fpc-information>
  <get-resource-monitor-fpc-slot-information>

show system rollback
  <get-rollback-information>

show system services
show system services dhcp
show system services dhcp binding
  <get-dhcp-binding-information>

show system services dhcp conflict
  <get-dhcp-conflict-information>

show system services dhcp global
  <get-dhcp-global-information>

show system services dhcp pool
  <get-dhcp-pool-information>

show system services dhcp statistics
  <get-dhcp-statistics-information>

show system services reverse
  <get-system-services-reverse-information>

show system services service-deployment
  <get-service-deployment-service-information>
```

```
show system snapshot
    <get-snapshot-information>

show system software
show system software backup
    <get-package-backup-information>
    <get-software-installation-status>
show system software recovery-package

show system statistics
    <get-statistics-information>

show system statistics bridge
    <get-system-bridge-statistics>
show system statistics extended
show system statistics vpls
show system storage
    <get-system-storage>
show system storage partitions
    <get-system-storage-partitions>
show system subscriber-management
show system subscriber-management route
    <get-subscriber-management-route>
show system subscriber-management route next-hop
    <get-subscriber-management-route-nh>
show system subscriber-management route summary
    <get-subscriber-management-route-summary>
show system subscriber-management statistics
    <get-subscriber-management-statistics>
show system subscriber-management summary
show system switchover
    <get-switchover-information>

show system uptime
    <get-system-uptime-information>

show system users
    <get-system-users-information>

show system virtual-memory
show task
show task io
show task logical-system-mux
    <get-lrmuxd-task-information>
show task logical-system-mux io
    <get-lrmuxd-tasks-io-statistics>
show task logical-system-mux memory
    <get-lrmuxd-task-memory>
show task memory
show task replication
    <get-routing-task-replication-state>
show task snooping
show task snooping io
show task snooping memory
    <get-snooping-task-memory-information>
show ted
show ted database
    <get-ted-database-information>

show ted link
    <get-ted-link-information>
```

```
show ted protocol
  <get-ted-protocol-information>
show unified-edge
show unified-edge gateways
show unified-edge ggsn-pgw
show unified-edge ggsn-pgw aaa
show unified-edge ggsn-pgw aaa network-element
show unified-edge ggsn-pgw aaa network-element status
show unified-edge ggsn-pgw aaa network-element-group
show unified-edge ggsn-pgw aaa network-element-group status
show unified-edge ggsn-pgw aaa radius
show unified-edge ggsn-pgw aaa radius statistics
show unified-edge ggsn-pgw aaa statistics
show unified-edge ggsn-pgw address-assignment
show unified-edge ggsn-pgw address-assignment group
show unified-edge ggsn-pgw address-assignment pool
show unified-edge ggsn-pgw address-assignment service-mode
show unified-edge ggsn-pgw address-assignment statistics
show unified-edge ggsn-pgw apn
show unified-edge ggsn-pgw apn service-mode
show unified-edge ggsn-pgw apn statistics
show unified-edge ggsn-pgw call-rate
show unified-edge ggsn-pgw call-rate statistics
show unified-edge ggsn-pgw charging
show unified-edge ggsn-pgw charging global
show unified-edge ggsn-pgw charging global statistics
show unified-edge ggsn-pgw charging local-persistent-storage
show unified-edge ggsn-pgw charging local-persistent-storage statistics
show unified-edge ggsn-pgw charging path
show unified-edge ggsn-pgw charging path statistics
show unified-edge ggsn-pgw charging path status
show unified-edge ggsn-pgw charging service-mode
show unified-edge ggsn-pgw charging transfer
show unified-edge ggsn-pgw charging transfer statistics
show unified-edge ggsn-pgw charging transfer status
show unified-edge ggsn-pgw charging trigger-profile
show unified-edge ggsn-pgw gtp
show unified-edge ggsn-pgw gtp peer
show unified-edge ggsn-pgw gtp peer count
show unified-edge ggsn-pgw gtp peer history
show unified-edge ggsn-pgw gtp peer statistics
show unified-edge ggsn-pgw gtp statistics
show unified-edge ggsn-pgw ip-reassembly
show unified-edge ggsn-pgw ip-reassembly statistics
show unified-edge ggsn-pgw resource-manager
show unified-edge ggsn-pgw resource-manager clients
show unified-edge ggsn-pgw service-mode
show unified-edge ggsn-pgw statistics
show unified-edge ggsn-pgw statistics traffic-class
show unified-edge ggsn-pgw status
show unified-edge ggsn-pgw status gtp-peer
show unified-edge ggsn-pgw status preemption-list
show unified-edge ggsn-pgw status session-state
show unified-edge ggsn-pgw subscribers
show unified-edge ggsn-pgw subscribers charging
show unified-edge ggsn-pgw subscribers traffic-class
show unified-edge ggsn-pgw system
show unified-edge ggsn-pgw system interfaces
show unified-edge ggsn-pgw system interfaces service-mode
show unified-edge sgw
```

```
show unified-edge sgw call-rate
show unified-edge sgw call-rate statistics
show unified-edge sgw charging
show unified-edge sgw charging global
show unified-edge sgw charging global statistics
show unified-edge sgw charging local-persistent-storage
show unified-edge sgw charging local-persistent-storage statistics
show unified-edge sgw charging path
show unified-edge sgw charging path statistics
show unified-edge sgw charging path status
show unified-edge sgw charging service-mode
show unified-edge sgw charging transfer
show unified-edge sgw charging transfer statistics
show unified-edge sgw charging transfer status
show unified-edge sgw charging trigger-profile
show unified-edge sgw gtp
show unified-edge sgw gtp peer
show unified-edge sgw gtp peer count
show unified-edge sgw gtp peer history
show unified-edge sgw gtp peer statistics
show unified-edge sgw gtp statistics
show unified-edge sgw idle-mode-buffering
show unified-edge sgw idle-mode-buffering statistics
show unified-edge sgw ip-reassembly
show unified-edge sgw ip-reassembly statistics
show unified-edge sgw resource-manager
show unified-edge sgw resource-manager clients
show unified-edge sgw service-mode
show unified-edge sgw statistics
show unified-edge sgw status
show unified-edge sgw status gtp-peer
show unified-edge sgw status preemption-list
show unified-edge sgw status session-state
show unified-edge sgw subscribers
show unified-edge sgw subscribers charging
show unified-edge sgw system
show unified-edge sgw system interfaces
show unified-edge sgw system interfaces service-mode
show version
    <get-software-information>

show virtual-chassis
show virtual-chassis active-topology
<get-virtual-chassis-active-topology>
show virtual-chassis device-topology
<get-virtual-chassis-device-topology>
show virtual-chassis fast-failover
<get-virtual-chassis-fast-failover>
show virtual-chassis heartbeat
<get-virtual-chassis-heartbeat-information>
show virtual-chassis login
<get-virtual-chassis-login>
show virtual-chassis mode
<get-virtual-chassis-mode-information>
show virtual-chassis protocol
show virtual-chassis protocol adjacency
<get-virtual-chassis-adjacency-information>
show virtual-chassis protocol database
<get-virtual-chassis-database-information>
show virtual-chassis protocol interface
<get-virtual-chassis-interface-information>
```

```
show virtual-chassis protocol route
<get-virtual-chassis-route-information>
show virtual-chassis protocol statistics
<get-virtual-chassis-statistics-information>
show virtual-chassis status
<get-virtual-chassis-information>
show virtual-chassis vc-path
<get-virtual-chassis-packet-path>
show virtual-chassis vc-port
<get-virtual-chassis-port-information>
show virtual-chassis vc-port diagnostics
show virtual-chassis vc-port diagnostics optics
<get-virtual-chassis-optics-diagnostics>
show virtual-chassis vc-port lag-hash
<get-virtual-chassis-port-lag-hash-information>
show virtual-chassis vc-port statistics
<get-virtual-chassis-port-statistics>
show vlans
<get-vlan-information>
show vlans operational
<get-operational-vlan-instance-information>

show vpls
show vpls connections
    <get-vpls-connection-information>

show vpls flood
show vpls flood event-queue
    <get-vpls-event-queue-information>

show vpls flood route
show vpls flood route all-ce-flood
    <get-vpls-all-ce-flood-route-information>

show vpls flood route all-flood
    <get-vpls-all-flood-route-information>

show vpls flood route alt-root-flood
    <get-vpls-alt-root-flood-route-information>

show vpls flood route ce-flood
    <get-vpls-ce-flood-route-information>

show vpls flood route mlp-flood
    <get-vpls-mlp-flood-route-information>

show vpls flood route re-flood
    <get-vpls-re-flood-route-information>

show vpls mac-table
    <get-vpls-mac-table>

show vpls mac-table interface
    <get-vpls-interface-mac-table>

show vpls statistics
    <get-vpls-statistics-information>

show vrrp
show vrrp interface
show vrrp track
```

```
test interface
test interface fd1-line-loop
test interface fd1-line-loop ansi
test interface fd1-line-loop ansi initiate
test interface fd1-line-loop ansi terminate
test interface fd1-line-loop bellcore
test interface fd1-line-loop bellcore initiate
test interface fd1-line-loop bellcore terminate
test interface fd1-payload-loop
test interface fd1-payload-loop ansi
test interface fd1-payload-loop ansi initiate
test interface fd1-payload-loop ansi terminate
test interface fd1-payload-loop bellcore
test interface fd1-payload-loop bellcore initiate
test interface fd1-payload-loop bellcore terminate
test interface inband-line-loop
test interface inband-line-loop ansi
test interface inband-line-loop ansi initiate
test interface inband-line-loop ansi terminate
test interface inband-line-loop bellcore
test interface inband-line-loop bellcore initiate
test interface inband-line-loop bellcore terminate
test interface inband-line-loop initiate
test interface inband-line-loop terminate
test interface inband-payload-loop
test interface inband-payload-loop ansi
test interface inband-payload-loop ansi initiate
test interface inband-payload-loop ansi terminate
test interface inband-payload-loop bellcore
test interface inband-payload-loop bellcore initiate
test interface inband-payload-loop bellcore terminate
test msdp
test msdp dependent-peers
test msdp rpf-peer
test policy
<
```

**Configuration
Hierarchy Levels**

```
[edit dynamic-profiles routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems services mobile-ip home-agent enable-service]
[edit routing-instances instance services mobile-ip home-agent enable-service]
[edit services mobile-ip home-agent enable-service]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 840](#)
- [Understanding Junos OS Access Privilege Levels on page 799](#)
- [Configuring Access Privilege Levels on page 829](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

view-configuration

Can view all of the configuration (not including secrets).

Commands No associated CLI commands.

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 840](#)
 - [Understanding Junos OS Access Privilege Levels on page 799](#)
 - [Configuring Access Privilege Levels on page 829](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 830](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 834](#)

Configuring Authentication Methods

- [Configuring RADIUS Server Authentication on page 1011](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 1014](#)
- [Configuring TACACS+ Authentication on page 1017](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)
- [Example: Configuring Authentication Order on page 1022](#)

Configuring RADIUS Server Authentication

RADIUS authentication is a method of authenticating users who attempt to access the router or switch.

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and that all vendors of these systems support RADIUS.

You should use RADIUS when your priorities are interoperability and performance:

- Interoperability—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
- Performance—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.

To use RADIUS authentication on the device, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server.

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. As such, the steps shown here are in a configuration group called **global**. Using a configuration group is optional.

To configure authentication by a RADIUS server:

1. Add an IPv4 or IPv6 server address.

- Configure an IPv4 source address and server address:

```
[edit groups global]
user@host# set system radius-server server-address source-address source-address
```

For example:

```
[edit groups global]
user@host# set system radius-server 192.168.17.28 source-address 192.168.17.1
```

- Configure an IPv6 source address and server address:

```
[edit groups global system radius-server server-address]
user@host# set server-address secret "secretkey" source-address source-address
```

For example:

```
[edit groups global system radius-server ::17.22.22.162]
user@host# set secret $9$ABC123 source-address ::17.22.22.1
```

The source address is a valid IPv4 or IPv6 address configured on one of the router or switch interfaces. This configuration sets a fixed address as the source address for locally generated IP packets.

Server address is a unique IPv4 or IPv6 address that is assigned to a particular server and used to route information to the server. If the Junos OS device has several interfaces that can reach the RADIUS server, assign an IP address that Junos OS can use for all its communication with the RADIUS server.

2. Include a shared secret password.

You must specify a password in the **secret *password*** statement. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router or switch must match that used by the server. The secret password configures the password that the Junos OS device uses to access the RADIUS server.

```
[edit groups global system radius-server server-address]
user@host# set secret password
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set secret $9$ABC123ABC123
```

3. If necessary, specify a port on which to contact the RADIUS server.

By default, port number 1812 is used (as specified in RFC 2865).



NOTE: You can also specify an accounting port to send accounting packets with the **accounting-port** statement. The default is 1813 (as specified in RFC 2866).

```
[edit groups global system radius-server server-address]
user@host# set port port-number
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set port 1845
```

4. Specify the order in which Junos OS attempts authentication.

You must include the **authentication-order** statement in your remote authentication configuration.

The example assumes your network includes both RADIUS and TACACS+ servers. In this example, whenever a user attempts to log in, Junos OS begins by querying the RADIUS server for authentication. If it fails, it next attempts authentication with locally configured user accounts. Finally the TACACS+ server is tried.

```
[edit groups global system]
user@host# set authentication-order [ authentication-methods ]
```

For example:

```
[edit groups global system]
user@host# set authentication-order [ radius password tacplus ]
```

5. Assign a login class to RADIUS-authenticated users.

You can assign different user templates and login classes to RADIUS-authenticated users. This allows RADIUS-authenticated users to be granted different administrative permissions on the Junos OS device. By default, RADIUS-authenticated users use the **remote** user template and are assigned to the associated class, which is specified in the **remote** user template, if the **remote** user template is configured. The username **remote** is a special case in Junos OS. It acts as a template for users who are authenticated by a remote server, but do not have a locally-configured user account on the device. In this method, Junos OS applies the permissions of the remote template to those authenticated users without a locally defined account. All users mapped to the remote template are of the same login class.

In the Junos OS configuration, a user template is configured in the same way as a regular local user account, except that no local authentication password is configured because the authentication is remotely performed on the RADIUS server.

- To use the same permissions for all RADIUS-authenticated users:

```
[edit groups global system login]
user@host# set user remote class class
```

For example:

```
[edit groups global system login]
user@host# set user remote class super-user
```

- To have different login classes be used for different RADIUS-authenticated users, granting them different permissions:
 - a. Create multiple user templates in the Junos OS configuration.

Every user template can be assigned a different login class.

For example:

```
[edit groups global system login]
```

```
set user RO class read-only
set user OP class operator
set user SU class super-user
set user remote full-name "default remote access user template"
set user remote class read-only
```

- b. Have the RADIUS server specify the name of the user template to be applied to the authenticated user.

For a RADIUS server to indicate which user template is to be applied, it needs to include the `Juniper-Local-User-Name` attribute (Vendor 2636, type 1, string) `Juniper VSA` (vendor-specific attribute) in the RADIUS Access-Accept message. The string value in the `Juniper-Local-User-Name` must correspond to the name of a configured user template on the device. For a list of relevant Juniper RADIUS VSAs, see [Juniper Networks Vendor-Specific RADIUS Attributes](#).

If the `Juniper-Local-User-Name` is not included in the Access-Accept message or the string contains a user template name that does not exist on the device, the user is assigned to the **remote** user template, if configured. If it is not configured, authentication fails for the user.

After logging in, the remotely authenticated user retains the same username that was used to log in. However, the user inherits the user class from the assigned user template.

In a RADIUS server, users can be assigned a `Juniper-Local-User-Name` string, which indicates the user template to be used in the Junos OS device. From the previous example, the string would be `RO`, `OP`, or `SU`.

Configuration of the RADIUS server depends on the server being used. For instructions for the Juniper Steel-Belted Radius server, see [Steel-Belted Radius \(SBR\) Enterprise](#). For information on using FreeRADIUS, see <http://kb.juniper.net/InfoCenter/index?page=content&id=KB19446>.

Example: Configuring a RADIUS Server for System Authentication

This example shows how to configure a RADIUS server for system authentication.

- [Requirements on page 1014](#)
- [Overview on page 1015](#)
- [Configuration on page 1015](#)
- [Verification on page 1016](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one RADIUS server. For more details, see [RADIUS Authentication and Accounting Servers Configuration Overview](#).

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1 and specify the shared secret password of the RADIUS server as Radiussecret1. The secret is stored as an encrypted value in the configuration database. Finally, you specify the source address to be included in the RADIUS server requests by the device. In most cases you can use the loopback address of the device, which in this example is 10.0.0.1.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system radius-server address 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the RADIUS section, click **Add**. The Add Radius Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the source IP address of the server.
9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see ["Using the CLI Editor in Configuration Mode" on page 434](#) in the *CLI User Guide*.

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.
[edit system]

```
user@host# set radius-server address 172.16.98.1
```

2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```

3. Specify the device's loopback address source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system radius-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system radius-server
radius-server 172.16.98.1 {
  secret Radiussecret1;
  source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 1022](#).
- Configure a user. See [“Example: Configuring New Users” on page 807](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 810](#).

Verification

Confirm that the configuration is working properly.

Verifying the RADIUS Server System Authentication Configuration

Purpose Verify that the RADIUS server has been configured for system authentication.

Action From operational mode, enter the **show system radius-server** command.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)

- [Understanding Login Classes on page 795](#)

Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

- [Configuring TACACS+ Server Details on page 1017](#)
- [Specifying a Source Address for the Junos OS to Access External TACACS+ Servers on page 1018](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 1018](#)
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 1019](#)

Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level:

```
[edit system]
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  timeout seconds;
}
```

server-address is the address of the TACACS+ server.

port-number is the TACACS+ server port number.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the **single-connection** statement.



NOTE: Early versions of the TACACS+ server do not support the **single-connection** option. If you specify this option and the server does not support it, the Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in *Overview of Template Accounts for RADIUS and TACACS+ Authentication*.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the **source-address** statement at the **[edit system tacplus-server server-address]** hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the **source-address** statement at the **[edit system accounting destination tacplus server server-address]** hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the **[edit system tacplus-server]** and **[edit system tacplus-options]** hierarchy levels. For information about how to configure a TACACS+ server at the **[edit system tacplus-server]** hierarchy level, see [“Configuring TACACS+ Authentication” on page 1017](#).

To assign the same authentication service to multiple TACACS+ servers, include the **service-name** statement at the **[edit system tacplus-options]** hierarchy level:

```
[edit system tacplus-options]
service-name service-name;
```

service-name is the name of the authentication service. By default, the service name is set to **junos-exec**.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
  10.2.2.2 secret "$ABC123"; ## SECRET-DATA
  10.3.3.3 secret "$ABC123"; ## SECRET-DATA
}
```

```

}
tacplus-options {
  service-name bob;
}

```

Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the Junos OS with TACACS+.

To specify these attributes, include a **service** statement of the following form in the TACACS+ server configuration file:

```

service = junos-exec {
  local-user-name = <username-local-to-router>
  allow-commands = "<allow-commands-regex>"
  allow-configuration-regexps = "<allow-configuration-regex>"
  deny-commands = "<deny-commands-regex>"
  deny-configuration-regexps = "<deny-configuration-regex>"
}

```

This **service** statement can appear in a **user** or **group** statement.

Related Documentation

- [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)

Example: Configuring a TACACS+ Server for System Authentication

This example shows how to configure a TACACS+ server for system authentication.

- [Requirements on page 1019](#)
- [Overview on page 1019](#)
- [Configuration on page 1020](#)
- [Verification on page 1021](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one TACACS+ server.

Overview

In this example, you set the IP address to 172.16.98.24 and the shared secret password of the TACACS+ server to Tacacssecret1. The secret password is stored as an encrypted value in the configuration database. You then set the loopback source address as 10.0.0.1

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system tacplus-server address 172.16.98.24
set system tacplus-server 172.16.98.24 secret Tacacssecret1
set system tacplus-server 172.16.98.24 source-address 10.0.0.1
```

GUI Step-by-Step Procedure To configure a TACACS+ server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the TACACS section, click **Add**. The Add TACACS Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the locally configured interface address, which is used as the source address for TACACS+ packets.



NOTE: The Source Address box can accept either a hostname or an IP address.

9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see ["Using the CLI Editor in Configuration Mode" on page 434](#) in the *CLI User Guide*.

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server address 172.16.98.24
```

2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 secret Tacacssecret1
```
3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system tacplus-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system tacplus-server
tacplus-server 172.16.98.24 {
  secret Tacacssecret1;
  source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 1022](#).
- Configure a user. See [“Example: Configuring New Users” on page 807](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 810](#).

Verification

Confirm that the configuration is working properly.

Verifying the TACACS+ Server System Authentication Configuration

Purpose Verify that the TACACS+ server has been configured for system authentication.

Action From operational mode, enter the **show system tacplus-server** command.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 1014](#)
- [Understanding Login Classes on page 795](#)

Example: Configuring Authentication Order

This example shows how to configure authentication order.

- [Requirements on page 1022](#)
- [Overview on page 1022](#)
- [Configuration on page 1022](#)
- [Verification on page 1023](#)

Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
 - RADIUS
 - TACACS+
 - Local Password

If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.

5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure authentication order:

1. Add RADIUS authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order radius after password
```
2. Add TACACS+ authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order tacplus after radius
```

Results From configuration mode, confirm your configuration by entering the **show system authentication-order** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system authentication-order
authentication-order [password, radius, tacplus];
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 1014](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 1019](#).
- Configure a user. See [“Example: Configuring New Users” on page 807](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 810](#).

Verification

Confirm that the configuration is working properly.

Verifying the Authentication Order Configuration

Purpose Verify that the authentication order has been configured.

Action From operational mode, enter the **show system authentication-order** command.

Related Documentation

- [Understanding User Authentication Methods on page 804](#)
- [Understanding User Accounts on page 798](#)
- [Understanding Login Classes on page 795](#)

PART 10

Configuring Remote Access to an SRX Series Appliances

- [Configuring Secure Web Access on page 1027](#)
- [Setting up USB Modems for Remote Management on page 1035](#)
- [Configuring Telnet and SSH Access to an SRX Series Appliance on page 1051](#)

Configuring Secure Web Access

- [Secure Web Access Overview on page 1027](#)
- [Generating an SSL Certificate Using the openssl Command on page 1028](#)
- [Generating a Self-Signed SSL Certificate on page 1028](#)
- [Manually Generating Self-Signed SSL Certificates on page 1029](#)
- [Configuring Device Addresses on page 1029](#)
- [Enabling Access Services on page 1030](#)
- [Example: Configuring Secure Web Access on page 1031](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 1033](#)

Secure Web Access Overview

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

**Related
Documentation**

- [Generating an SSL Certificate Using the openssl Command on page 1028](#)
- [Generating a Self-Signed SSL Certificate on page 1028](#)
- [Configuring Device Addresses on page 1029](#)
- [Example: Configuring Secure Web Access on page 1031](#)

Generating an SSL Certificate Using the openssl Command

To generate an SSL certificate using the **openssl** command:

1. Enter **openssl** in the CLI. The **openssl** command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.



NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the **openssl** command.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out  
filename.pem
```

Replace **filename** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file **new.pem**.

```
cat new.pem
```

Copy the contents of this file for installing the SSL certificate.

**Related
Documentation**

- [Secure Web Access Overview on page 1027](#)

Generating a Self-Signed SSL Certificate

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

```
user@host> request system reboot  
Reboot the system ? [yes,no] yes
```

3. Specify **system-generated-certificate** under HTTPS Web management.

```
[edit]
user@host# show system services web-management https
system-generated-certificate
```

Related Documentation • [Generating an SSL Certificate Using the openssl Command on page 1028](#)

Manually Generating Self-Signed SSL Certificates

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:

```
root@host> request security pki generate-size 512 certificate-id certname
```

Generated key pair *sslcert*, key size 512 bits

```
root@host> request security pki local-certificate generate-self-signed certificate-id
cert-name email email domain-name domain-name ip-address ip-address subject
"DC= Domain name, CN= Common-Name, OU= Organizational-Unit-name, O=
Organization-Name, ST= state, C= Country"
```

Self-signed certificate generated and loaded successfully



NOTE: When generating the certificate, you must specify the subject, e-mail address, and either domain-name or ip-address.

3. Specify **local-certificate** under HTTPS Web management.

```
[edit]
root@host# show system services web-management https local-certificate certname
```

Related Documentation • [Generating a Self-Signed SSL Certificate on page 1028](#)

Configuring Device Addresses

You can use the Management tab to configure IPv4 and loopback addresses on the device.

To configure IPv4 and loopback addresses:

1. In the J-Web user interface, select **Configure > System Properties > Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Management** tab.
4. If you want to enable a loopback address for the device, enter an address and corresponding subnet mask in the **Loopback address** section.

5. If you want to enable an IPv4 address for the device, select **IPv4 address** and enter a corresponding management port, subnet mask, and default gateway.
6. Click **OK** to save the configuration or **Cancel** to clear it.

Related Documentation

- [Enabling Access Services on page 1030](#)

Enabling Access Services

You can use the Services tab to specify the type of connections that users can make to the device. For instance, you can enable secure HTTPS sessions to the device or enable access to the Junos XML protocol XML scripting API.

To enable access services:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Services** tab.
4. If you want to enable users to create secure Telnet or secure SSH connections to the device, select **Enable Telnet** or **Enable SSH**.
5. If you want to enable access to the Junos XML protocol XML scripting API, select **Enable Junos XML protocol over clear text** or **Enable Junos XML protocol over SSL**. If you enable Junos XML protocol over SSL, select the certificate you want to use for encryption from the **Junos XML protocol certificate** drop-down list.
6. Select **Enable HTTP** if you want users to connect to device interfaces over an HTTP connection. Then specify the interfaces that should use the HTTP connection:
 - **Enable on all interfaces**—Select this option if you want to enable HTTP on all device interfaces.
 - **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTP on only some of the device interfaces.
7. If you want users to connect to device interfaces over a secure HTTPS connection, select **Enable HTTPS**. Then select which certificate you want to use to secure the connection from the **HTTPS certificates** list and specify the interfaces that should use the HTTPS connection:
 - **Enable on all interfaces**—Select this option if you want to enable HTTPS on all device interfaces.
 - **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTPS on only some of the device interfaces.
8. Click **OK** to save the configuration or **Cancel** to clear it.

To verify that Web access is enabled correctly, connect to the device using one of the following methods:

- For HTTP access—In your Web browser, type **http://URL** or **http://IP address**.

- For HTTPS access—In your Web browser, type **https://URL** or **https://IP address**.
- For SSL Junos XML protocol access—A Junos XML protocol client such as Junos Scope is required.

Related Documentation

- [Configuring Device Addresses on page 1029](#)

Example: Configuring Secure Web Access

This example shows how to configure secure Web access on your device.

- [Requirements on page 1031](#)
- [Overview on page 1031](#)
- [Configuration on page 1031](#)
- [Verification on page 1032](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.



NOTE: You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.

Overview

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

```
[edit security]
user@host# set certificates local new load-key-file /var/tmp/new.pem
```

2. Enable HTTPS access and specify the SSL certificate and port.

```
[edit system]
user@host# set services web-management https local-certificate new port 8443
```

Results From configuration mode, confirm your configuration by entering the **show security** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
certificates {
  local {
    new {
      "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQC/C5UI4frNqbi
      qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY
      Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXl4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
      ... KYiFf4CbBBbjlMQJOHFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
      eIQBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
      CERTIFICATE----- \nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
      FADCBkTELMakGAiUEBhMCdXMx\nCzAJBgNVBAGTAhNhmMRiWEAYDVQQHEwldW5ue
      HBIYnMxDTALBgNVBAMTBGpucHlxJDAiBgkqhkiG\n9w0BCQEWFW5iaGFyZ2F2YUB
      fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying an SSL Certificate Configuration on page 1032](#)
- [Verifying a Secure Access Configuration on page 1032](#)

Verifying an SSL Certificate Configuration

Purpose Verify the SSL certificate configuration.

Action From operational mode, enter the **show security** command.

Verifying a Secure Access Configuration

Purpose Verify the secure access configuration.

Action From operational mode, enter the **show system services** command. The following sample output displays the sample values for secure Web access:

```
[edit]
```



```

user@host# show system services
web-management {
  http;
  https {
    port 8443;
    local-certificate new;
  }
}

```

Related Documentation

- [Secure Web Access Overview on page 1027](#)
- [Generating an SSL Certificate Using the openssl Command on page 1028](#)
- [Generating a Self-Signed SSL Certificate on page 1028](#)
- [Configuring Device Addresses on page 1029](#)

Adding, Editing, and Deleting Certificates on the Device

You can use the Certificates tab to upload SSL certificates to the device, edit existing certificates on the device, or delete certificates from the device. You can use the certificates to secure HTTPS and Junos XML protocol sessions.

To add, edit, or delete a certificate:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Certificates** tab.
4. Choose one of the following options:
 - If you want to add a new certificate, click **Add**. The Add Certificate section is expanded.
 - If you want to edit the information for an existing certificate, select it and click **Edit**. The Edit Certificate section is expanded.
 - If you want to delete an existing certificate, select it and click **Delete**. (You can skip the remaining steps in this section.)
5. In the **Certificate Name** box, type a name—for example, **new**.
6. In the **Certificate content** box, paste the generated certificate and RSA private key.
7. Click **Save**.
8. Click **OK** to save the configuration or **Cancel** to clear it.

Related Documentation

- [Generating an SSL Certificate Using the openssl Command on page 1028](#)

Setting up USB Modems for Remote Management

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Example: Configuring a USB Modem Interface on page 1040](#)
- [Example: Configuring a Dialer Interface on page 1042](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 1046](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 1048](#)
- [Connecting to the Device Remotely on page 1049](#)
- [Modifying USB Modem Initialization Commands on page 1049](#)
- [Resetting USB Modems on page 1050](#)

USB Modem Interface Overview

Juniper Networks devices support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

You can configure your device to fail over to a USB modem connection when the primary Internet connection experiences interruption.

A USB modem connects to a device through modem interfaces that you configure. The device applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the device and the modem at the user end of the network.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.



NOTE: Low-latency traffic such as VoIP traffic is not supported over USB modem connections.



NOTE: We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity:

- A physical interface which uses the naming convention **umdn0**. The device creates this interface when a USB modem is connected to the USB port.
- A logical interface called the dialer interface. You use the dialer interface, **dln**, to configure dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP). You can configure multiple dialer interfaces for different functions on the device. After configuring the dialer interface, you must configure a backup method such as a dialer backup, a dialer filter, or a dialer watch.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface. Dialer pool priority has a range from 1 to 255, with 1 designating the lowest priority interfaces and 255 designating the highest priority interfaces.

Dialer Interface Rules

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- The dialer interface cannot be configured as a constituent link in a multilink bundle.
- The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
 - As a backup interface—for one primary interface
 - As a dialer filter
 - As a dialer watch interface

The backup dialer interfaces are activated only when the primary interface fails. USB modem backup connectivity is supported on all interfaces except `lsq-0/0/0`.

The dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed. You define an interesting packet using the dialer filter feature of the device. To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route. If the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

How the Device Initializes USB Modems

When you connect the USB modem to the USB port on the device, the device applies the modem AT commands configured in the **init-command-string** command to the initialization commands on the modem.

If you do not configure modem AT commands for the **init-command-string** command, the device applies the following default sequence of initialization commands to the modem: **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. [Table 79](#) describes the commands. For more information about these commands, see the documentation for your modem.

Table 79: Default Modem Initialization Commands

Modem Command	Description
AT	Attention. Informs the modem that a command follows.
S7=45	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
S0=0	Disables the auto answer feature, whereby the modem automatically answers calls.
V1	Displays result codes as words.
&C1	Disables reset of the modem when it loses the carrier signal.
E0	Disables the display on the local terminal of commands issued to the modem from the local terminal.
Q0	Enables the display of result codes.
&Q8	Enables Microcom Networking Protocol (MNP) error control mode.
%C0	Disables data compression.

When the device applies the modem AT commands in the **init-command-string** command or the default sequence of initialization commands to the modem, it compares them to

the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include **S0=0** and the device's **init-command-string** command includes **S0=2**, the device applies **S0=2**.
- If the initialization commands on the modem do not include a command in the device's **init-command-string** command, the device adds it. For example, if the **init-command-string** command includes the command **L2**, but the modem commands do not include it, the device adds **L2** to the initialization commands configured on the modem.

**Related
Documentation**

- [USB Modem Configuration Overview on page 1038](#)
- [Example: Configuring a USB Modem Interface on page 1040](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 1046](#)

USB Modem Configuration Overview

Before you begin:

1. Install device hardware. For more information, see the Getting Started Guide for your device.
2. Establish basic connectivity. For more information, see the Getting Started Guide for your device.
3. Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637 (<http://www.usr.com/>).
4. Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
5. Connect the USB modem to the device's USB port.



NOTE: When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

- a. Plug the modem into the USB port.
- b. Connect the modem to your telephone network.

Suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. This example shows you how to establish a backup connection between the branch office and head office routers. See [Table 80](#) for a summarized description of the procedure.

Table 80: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity

Router Location	Configuration Requirement	Procedure
Branch Office	Configure the logical dialer interface on the branch office router for USB modem dial backup.	To configure the logical dialer interface, see "Example: Configuring a USB Modem Interface" on page 1040.
	Configure the dialer interface dl0 on the branch office router using one of the following backup methods: <ul style="list-style-type: none"> Configure the dialer interface dl0 as the backup interface on the branch office router's primary T1 interface t1-1/0/0. Configure a dialer filter on the branch office router's dialer interface. Configure a dialer watch on the branch office router's dialer interface. 	Configure the dialer interface using one of the following backup methods: <ul style="list-style-type: none"> To configure dl0 as a backup for t1-1/0/0 see <i>Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</i>. To configure a dialer filter on dl0, see <i>Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</i>. To configure a dialer watch on dl0, see <i>Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</i>.
Head Office	Configure dial-in on the dialer interface dl0 on the head office router.	To configure dial-in on the head office router, see "Example: Configuring a Dialer Interface for USB Modem Dial-In" on page 1046.

If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085321091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

See [Table 81](#) for a list of available incoming map options.

Table 81: Incoming Map Options

Option	Description
accept-all	Dialer interface accepts all incoming calls. You can configure the accept-all option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the accept-all option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

Table 81: Incoming Map Options (*continued*)

Option	Description
caller	<p>Dialer interface accepts calls from a specific caller ID. You can configure a maximum of 15 caller IDs per dialer interface.</p> <p>The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.</p>

You configure dialer interfaces to support PAP. PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair are repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

**Related
Documentation**

- [USB Modem Interface Overview on page 1035](#)
- [Example: Configuring a USB Modem Interface on page 1040](#)

Example: Configuring a USB Modem Interface

This example shows how to configure a USB modem interface for dial backup.

- [Requirements on page 1040](#)
- [Overview on page 1040](#)
- [Configuration on page 1040](#)
- [Verification on page 1041](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you create an interface called as umd0 for USB modem connectivity and set the dialer pool priority to 25. You also configure a modem initialization string to autoanswer after a specified number of rings. The default modem initialization string is **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. The modem command **S0=0** disables the modem from autoanswering the calls. Finally, you set the modem to act as a dial-in WAN backup interface.

Configuration

**CLI Quick
Configuration**

To quickly configure this example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the command into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
```



```
set modem-options init-command-string "ATSO=2 \n" dialin routable
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure a USB modem interface for dial backup:

1. Create an interface.

```
[edit]
user@host# edit interfaces umd0
```
2. Set the dialer options and priority.

```
[edit interfaces umd0]
user@host# set dialer-options pool usb-modem-dialer-pool priority 25
```
3. Specify the modem options.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "ATSO=2 \n"
```
4. Set the modem to act as a dial-in WAN backup interface.

```
[edit interfaces umd0]
user@host# set modem-options dialin routable
```

Results From configuration mode, confirm your configuration by entering the **show interface umd0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interface umd0
modem-options {
  init-command-string "ATSO=2 \n";
  dialin routable;
}
dialer-options {
  pool usb-modem-dialer-pool priority 25;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose Verify a USB modem interface for dial backup.

Action From configuration mode, enter the **show interfaces umd0 extensive** command. The output shows a summary of interface information and displays the modem status.

```
Physical interface:  umd0, Enabled, Physical link is Up
```

```
Interface index:      64, SNMP ifIndex: 33, Generation: 1
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
Clocking: Unspecified, Speed: MODEM
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags     : None
Hold-times     : Up 0 ms, Down 0 ms
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes  :          21672
  Output bytes :          22558
  Input packets:           1782
  Output packets:          1832
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
  Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
MODEM status:
  Modem type                : LT V.92 1.0 MT5634ZBA-USB-V92 Data/Fax Modem

(Dual Config) Version 2.27m
  Initialization command string : AT$0=2
  Initialization status         : Ok
  Call status                    : Connected to 4085551515
  Call duration                  : 13429 seconds
  Call direction                 : Dialin
  Baud rate                      : 33600 bps
  Most recent error code         : NO CARRIER

Logical interface umd0.0 (Index 2) (SNMP ifIndex 34) (Generation 1)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP-Subordinate
```

- Related Documentation**
- [USB Modem Configuration Overview on page 1038](#)
 - [USB Modem Interface Overview on page 1035](#)
 - [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 1046](#)

Example: Configuring a Dialer Interface

This example shows how to configure a logical dialer interface for the device.

- [Requirements on page 1042](#)
- [Overview on page 1043](#)
- [Configuration on page 1043](#)
- [Verification on page 1045](#)

Requirements

Before you begin:

- Install device hardware and establish basic connectivity. See the Getting Started Guide for your device.
- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637, from US Robotics (<http://www.usr.com/>).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the device.
- Order a PSTN line from your telecommunications service provider. Contact your service provider.

Overview

In this example, you configure a logical dialer interface called `dl0` to establish USB connectivity. You can configure multiple dialer interfaces for different functions on the device. You add a description to differentiate among different dialer interfaces. For example, this modem is called `USB-modem-remote-management`. Configure PPP encapsulation and set the logical unit as 0. You then specify the name of the dialer pool as `usb-modem-dialer-pool` and set the source and destination IP addresses as 172.20.10.2, and 172.20.10.1, respectively.



NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.



NOTE: If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces dl0 description USB-modem-remote-management encapsulation ppp
set interfaces dl0 unit 0 dialer-options pool usb-modem-dialer-pool
set interfaces dl0 unit 0 family inet address 172.20.10.2 destination 172.20.10.1
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure a logical dialer interface for the device:

1. Create an interface.

```
[edit]
user@host# set interfaces dl0
```

2. Add a description and configure PPP encapsulation.

```
[edit interfaces dl0]
user@host# set description USB-modem-remote-management
user@host# set encapsulation ppp
```

3. Create the logical unit.



NOTE: The logical unit number must be 0.

```
[edit interfaces dl0]
user@host# set unit 0
```

4. Configure the name of the dialer pool to use for USB modem connectivity.

```
[edit interfaces dl0 unit 0]
user@host# set dialer-options pool usb-modem-dialer-pool
```

5. Configure source and destination IP addresses for the dialer interface.

```
[edit interfaces dl0 unit 0]
user@host# set family inet address 172.20.10.2 destination 172.20.10.1
```

Results From configuration mode, confirm your configuration by entering the **show interfaces dl0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces dl0
description USB-modem-remote-management;
encapsulation ppp;
unit 0 {
  family inet {
    address 172.20.10.2/32 {
      destination 172.20.10.1;
    }
  }
  dialer-options {
    pool usb-modem-dialer-pool;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying a Dialer Interface

Purpose Verify that the dialer interface has been configured.

Action From configuration mode, enter the **show interfaces d10 extensive** command. The output shows a summary of dialer interface information.

```
Physical interface: d10, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
  Device flags      : Present Running
  Interface flags:  SNMP-Traps
  Link type        : Full-Duplex
  Link flags       : Keepalives
  Physical info    : Unspecified
  Hold-times       : Up 0 ms, Down 0 ms
  Current address:  Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped     : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes  :                13859                0 bps
    Output bytes :                   0                0 bps
    Input packets:                 317                0 pps
    Output packets:                  0                0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
  Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0

Logical interface d10.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
  Description: USB-modem-remote-management
  Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
  Dialer:
    State: Active, Dial pool: usb-modem-dialer-pool
    Dial strings: 220
    Subordinate interfaces: umd0 (Index 64)
    Activation delay: 0, Deactivation delay: 0
    Initial route check delay: 120
    Redial delay: 3
    Callback wait period: 5
    Load threshold: 0, Load interval: 60
  Bandwidth: 115200
  Traffic statistics:
    Input bytes  :                24839
    Output bytes :                17792
    Input packets:                 489
    Output packets:                 340
  Local statistics:
    Input bytes  :                10980
    Output bytes :                17792
```

```
Input packets:          172
Output packets:         340
Transit statistics:
Input bytes  :          13859          0 bps
Output bytes :           0          0 bps
Input packets:         317          0 pps
Output packets:         0          0 pps
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Success
  Protocol inet, MTU: 1500, Generation: 136, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 172.20.10.1, Local: 172.20.10.2, Broadcast: Unspecified,
    Generation: 134
```

**Related
Documentation**

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Example: Configuring a USB Modem Interface on page 1040](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 1046](#)

Example: Configuring a Dialer Interface for USB Modem Dial-In

This example shows how to configure a dialer interface for USB modem dial-in.

- [Requirements on page 1046](#)
- [Overview on page 1046](#)
- [Configuration on page 1047](#)
- [Verification on page 1047](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the system matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the system performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID

configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

You can configure the following incoming map options for the dialer interface:

- **accept-all**—Dialer interface accepts all incoming calls.

You can configure the **accept-all** option for only one of the dialer interfaces associated with a USB modem physical interface. The device uses the dialer interface with the **accept-all** option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

- **caller**—Dialer interface accepts calls from a specific caller ID—for example, **4085550115**. You can configure a maximum of 15 caller IDs per dialer interface.

The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.

In this example, you configure the incoming map option as caller 4085550115 for dialer interface d10.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the command into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces d10 unit 0 dialer-options incoming-map caller 4085550115
```

Step-by-Step Procedure

To configure a dialer interface for USB modem dial-in:

1. Select a dialer interface.

```
[edit]
user@host# edit interfaces d10
```
2. Configure the incoming map options.

```
[edit]
user@host# edit unit 0 dialer-options incoming-map caller 4085551515
```
3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show interface d10** command.

Related Documentation

- [USB Modem Configuration Overview on page 1038](#)
- [Example: Configuring a USB Modem Interface on page 1040](#)

Configuring a Dial-Up Modem Connection Remotely

To remotely connect to the USB modem connected to the USB port on the device, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection remotely:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. Connect the modem to your telephone network.
3. On the PC or laptop computer, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
4. Click **Create a new connection**. The New Connection Wizard appears.
5. Click **Next**. The New Connection Wizard: Network Connection Type page appears.
6. Select **Connect to the network at my workplace**, and then click **Next**.
The New Connection Wizard: Network Connection page appears.
7. Select **Dial-up connection**, and then click **Next**. The New Connection Wizard: Connection Name page appears.
8. In the Company Name box, type the dial-up connection name, for example **USB-modem-connect**. Then, click **Next**. The New Connection Wizard: Phone Number to Dial page appears.
9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the device end.
10. Click **Next** twice, and then click **Finish**. The Connect USB-modem-connect page appears.
11. If CHAP is configured on the dialer interface used for the USB modem interface at the device end, type the username and password configured in the CHAP configuration in the User name and Password boxes.
12. Click **Properties**. The USB-modem-connect Properties page appears.
13. In the Networking tab, select **Internet Protocol (TCP/IP)**, and then click **Properties**. The Internet Protocol (TCP/IP) Properties page appears.
14. Click **Advanced**. The Advanced TCP/IP Settings page appears.
15. Clear the **Use IP header compression** check box.

Related Documentation

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Connecting to the Device Remotely on page 1049](#)

Connecting to the Device Remotely

To remotely connect to the device through a USB modem connected to the USB port on the device:

1. On the PC or laptop computer at your remote location, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
2. Double-click the **USB-modem-connect** dial-up connection. The Connect USB-modem-connect page appears.
3. Click **Dial** to connect to the Juniper Networks device.

When the connection is complete, you can use Telnet or SSH to connect to the device.

Related Documentation

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 1048](#)

Modifying USB Modem Initialization Commands



NOTE: These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands.

You can use the CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.



NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.

You can configure the following modem AT commands to initialize the USB modem:

- The command **S0=2** configures the modem to automatically answer calls on the second ring.
- The command **L2** configures medium speaker volume on the modem.

You can insert spaces between commands.

When you configure modem commands in the CLI configuration editor, you must follow these conventions:

- Use the newline character `\n` to indicate the end of a command sequence.

- Enclose the command string in double quotation marks.

You can override the value of the **S0=0** command in the initialization sequence configured on the modem and add the **L2** command.

To modify the initialization commands on a USB modem:

1. Configure the modem AT commands to initialize the USB modem.

```
[edit interfaces umd0]
```

```
user@host# set modem-options init-command-string "AT S0=2 L2 \n"
```

2. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Resetting USB Modems on page 1050](#)

Resetting USB Modems

If the USB modem does not respond, you can reset the modem.



CAUTION: If you reset the modem when a call is in progress, the call is terminated.

To reset the USB modem, in operational mode, enter the following command:

```
user@host> request interface modem reset umd0
```

**Related
Documentation**

- [USB Modem Interface Overview on page 1035](#)
- [USB Modem Configuration Overview on page 1038](#)
- [Modifying USB Modem Initialization Commands on page 1049](#)

Configuring Telnet and SSH Access to an SRX Series Appliance

- [Securing the Console Port Configuration Overview on page 1051](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 1052](#)
- [Configuring Reverse Telnet and Reverse SSH on page 1053](#)
- [Example: Controlling Management Access on SRX Series Devices on page 1054](#)
- [Example: Configuring a Filter to Block Telnet and SSH Access on page 1057](#)
- [The telnet Command on page 1062](#)
- [The ssh Command on page 1063](#)
- [Configuring Outbound SSH Service on page 1064](#)

Securing the Console Port Configuration Overview

You can use the console port on the device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:

- Log out of the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to the console. This action prevents a non-root user from performing password recovery operation using the console.
- Disable the console port. We recommend disabling the console port to prevent unauthorized access to the device, especially when the device is used as customer premises equipment (CPE) and is forwarding sensitive traffic.



NOTE: It is not always possible to disable the console port, because console access is important during operations such as software upgrades.

To secure the console port:

1. Do one of the following:

- Disable the console port. Enter

```
[edit system ports console]  
user@host# set disable
```

- Disable root login connections to the console. Enter

```
[edit system ports console]  
user@host# set insecure
```



NOTE: After configuring the console port as insecure, if a user tries to perform password recovery operation by booting in single-user mode, the device will prompt for the root password. This way, the user will be unable to log in to single-user mode for password recovery unless the root password is known.

- Log out the console session when the serial cable connected to the console port is unplugged. Enter

```
[edit system ports console]  
user@host# set log-out-on-disconnect
```

2. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [The telnet Command on page 1062](#)
- [The ssh Command on page 1063](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 1052](#)
- [Configuring Reverse Telnet and Reverse SSH on page 1053](#)

Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.

For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.

- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
- Enforce a minimum session time of 40 seconds during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is **10**, but you can set a number from 1 through 10.

```
[edit system login retry-options]  
user@host# set tries-before-disconnect 4
```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is **2**, but you can specify a value from 1 through 3.

```
[edit system login retry-options]  
user@host# set backoff-threshold 2
```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of **5** seconds, but you can specify a value from 5 through 10 seconds.

```
[edit system login retry-options]  
user@host# set backoff-factor 5
```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is **20** seconds, but you can specify an interval from 20 through 60 seconds.

```
[edit system login retry-options]  
user@host# set minimum-time 40
```

5. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [The telnet Command on page 1062](#)
- [The ssh Command on page 1063](#)
- [Configuring Reverse Telnet and Reverse SSH on page 1053](#)

Configuring Reverse Telnet and Reverse SSH

To configure reverse telnet and reverse ssh:

1. Enable reverse telnet.

```
[edit]  
user@host# set system services reverse telnet
```

2. Specify the port to be used for reverse telnet. If you do not specify a port, 2900 is the default port that is used.

[edit]

user@host# **set system services reverse telnet port 5000**

3. Enable reverse ssh to encrypt the connection between the device and the client.

[edit]

user@host# **set system services reverse ssh**

4. Specify the port for reverse ssh. If you do not specify a port, 2901 is the default port that is used.

[edit]

user@host# **set system services reverse ssh port 6000**

5. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [The telnet Command on page 1062](#)
- [The ssh Command on page 1063](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 1052](#)

Example: Controlling Management Access on SRX Series Devices

This example shows how to control management access on SRX Series devices.

- [Requirements on page 1054](#)
- [Overview on page 1054](#)
- [Configuration on page 1054](#)
- [Verification on page 1057](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

By default, any host on the trusted interface can manage a security device. To limit the IP addresses that can manage a device, you can configure a firewall filter to deny all, with the exception of the IP address or addresses to which you want to grant management access. This example shows how to limit management access to a specific IP addresses to allow it to manage SRX Series devices.

Configuration

- [Configuring an IP Address List to Restrict Management Access to a Device on page 1054](#)

Configuring an IP Address List to Restrict Management Access to a Device

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```

set policy-options prefix-list manager-ip 192.168.4.254/32
set policy-options prefix-list manager-ip 10.0.0.0/8
set firewall filter manager-ip term block_non_manager from source-address 0.0.0.0/0
set firewall filter manager-ip term block_non_manager from source-prefix-list manager-ip
except
set firewall filter manager-ip term block_non_manager from protocol tcp
set firewall filter manager-ip term block_non_manager from destination-port ssh
set firewall filter manager-ip term block_non_manager from destination-port https
set firewall filter manager-ip term block_non_manager from destination-port telnet
set firewall filter manager-ip term block_non_manager from destination-port http
set firewall filter manager-ip term block_non_manager then discard
set firewall filter manager-ip term accept_everything_else then accept
set interfaces lo0 unit 0 family inet filter input manager-ip

```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

1. Define a set of host addresses, called "manager-ip", that are allowed to manage the device.

```

[edit policy-options]
user@host# set prefix-list manager-ip 192.168.4.254/32
user@host# set prefix-list manager-ip 10.0.0.0/8

```



NOTE: The configured list is referenced in the actual filter, where you can change your defined set of addresses.

2. Configure a firewall filter to deny traffic from all IP addresses except the IP addresses defined in the "manager-ip" list. Management traffic that uses any of the listed destination ports is rejected when the traffic comes from an address in the list.

```

[edit firewall filter]
user@host# set manager-ip term block_non_manager from source-address 0.0.0.0/0
user@host# set manager-ip term block_non_manager from source-prefix-list
manager-ip except
user@host# set manager-ip term block_non_manager from protocol tcp
user@host# set manager-ip term block_non_manager from destination-port ssh
user@host# set manager-ip term block_non_manager from destination-port https
user@host# set manager-ip term block_non_manager from destination-port telnet
user@host# set manager-ip term block_non_manager from destination-port http
user@host# set manager-ip term block_non_manager then discard
user@host# set manager-ip term accept_everything_else then accept

```

3. Apply stateless firewall filters to the loopback interface to filter the packets originating from the hosts to which you are granting management access.

```

[edit interfaces lo0 unit 0 ]
user@host# set family inet filter input manager-ip

```



NOTE: This configuration applies to traffic that terminates at the device. For traffic that terminates at the device interface (such as IPsec, OSPF, RIP, or BGP), you must also include the management IP addresses in the `manager-ip` prefix-list.

Results From configuration mode, confirm your configuration by entering **show configuration** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

user@host# show configuration policy-options
  prefix-list manager-ip {
    10.0.0.0/8;
    192.168.4.254/32;
  }

user@host# show configuration firewall
  filter manager-ip {
    term block_non_manager {
      from {
        source-address {
          0.0.0.0/0;
        }
        source-prefix-list {
          manager-ip except;
        }
      }
      protocol tcp;
      destination-port [ ssh https telnet http ];
    }
    then {
      discard;
    }
  }
  term accept_everything_else {
    then accept;
  }
}

user@host# show configuration interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input manager-ip;
      }
    }
  }
}

user@host# show configuration interfaces lo0
unit 0 {
  family inet {
    filter {

```



```
        input manager-ip;
    }
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Interfaces

Purpose Verify if the interfaces are configured correctly.

Action From operational mode, enter the following commands:

- show policy-options
- show firewall
- show interfaces

Related Documentation

- [Securing the Console Port Configuration Overview on page 1051](#)

Example: Configuring a Filter to Block Telnet and SSH Access

- [Requirements on page 1057](#)
- [Overview on page 1057](#)
- [Configuration on page 1058](#)
- [Verification on page 1060](#)

Requirements

You must have access to a remote host that has network connectivity with this device.

Overview

In this example, you create an IPv4 stateless firewall filter that logs and rejects Telnet or SSH access packets unless the packet is destined for or originates from the 192.168.1.0/24 subnet.

- To match packets destined for or originating from the **address 192.168.1.0/24** subnet, you use the **address 192.168.1.0/24** IPv4 match condition.
- To match packets destined for or originating from a TCP port, Telnet port, or SSH port, you use the **protocol tcp**, **port telnet**, and **telnet ssh** IPv4 match conditions.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To configure this example, perform the following tasks:

- [Configure the Stateless Firewall Filter on page 1058](#)
- [Apply the Firewall Filter to the Loopback Interface on page 1059](#)
- [Confirm and Commit Your Candidate Configuration on page 1059](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set firewall family inet filter local_acl term terminal_access from address 192.168.1.0/24
set firewall family inet filter local_acl term terminal_access from protocol tcp
set firewall family inet filter local_acl term terminal_access from port ssh
set firewall family inet filter local_acl term terminal_access from port telnet
set firewall family inet filter local_acl term terminal_access then accept
set firewall family inet filter local_acl term terminal_access_denied from protocol tcp
set firewall family inet filter local_acl term terminal_access_denied from port ssh
set firewall family inet filter local_acl term terminal_access_denied from port telnet
set firewall family inet filter local_acl term terminal_access_denied then log
set firewall family inet filter local_acl term terminal_access_denied then reject
set firewall family inet filter local_acl term default-term then accept
set interfaces lo0 unit 0 family inet filter input local_acl
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Configure the Stateless Firewall Filter

Step-by-Step Procedure

To configure the stateless firewall filter that selectively blocks Telnet and SSH access:

1. Create the stateless firewall filter **local_acl**.

```
[edit]
user@myhost# edit firewall family inet filter local_acl
```

2. Define the filter term **terminal_access**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access from address 192.168.1.0/24
user@myhost# set term terminal_access from protocol tcp
user@myhost# set term terminal_access from port ssh
user@myhost# set term terminal_access from port telnet
user@myhost# set term terminal_access then accept
```

3. Define the filter term **terminal_access_denied**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access_denied from protocol tcp
user@myhost# set term terminal_access_denied from port ssh
user@myhost# set term terminal_access_denied from port telnet
```

```

user@myhost# set term terminal_access_denied then log
user@myhost# set term terminal_access_denied then reject
user@myhost# set term default-term then accept

```

Apply the Firewall Filter to the Loopback Interface

Step-by-Step Procedure

- To apply the firewall filter to the loopback interface:

```

[edit]
user@myhost# set interfaces lo0 unit 0 family inet filter input local_acl
user@myhost# set interfaces lo0 unit 0 family inet address 127.0.0.1/32

```

Confirm and Commit Your Candidate Configuration

Step-by-Step Procedure

To confirm and then commit your candidate configuration:

1. Confirm the configuration of the stateless firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

[edit]
user@myhost# show firewall
family inet {
  filter local_acl {
    term terminal_access {
      from {
        address {
          192.168.1.0/24;
        }
        protocol tcp;
        port [ssh telnet];
      }
      then accept;
    }
    term terminal_access_denied {
      from {
        protocol tcp;
        port [ssh telnet];
      }
      then {
        log;
        reject;
      }
    }
    term default-term {
      then accept;
    }
  }
}

```

2. Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

[edit]

```

```
user@myhost# show interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input local_acl;
      }
      address 127.0.0.1/32;
    }
  }
}
```

3. If you are done configuring the device, commit your candidate configuration.

```
[edit]
user@myhost# commit
```

Verification

Confirm that the configuration is working properly.

- [Verifying Accepted Packets on page 1060](#)
- [Verifying Logged and Rejected Packets on page 1061](#)

Verifying Accepted Packets

Purpose Verify that the actions of the firewall filter terms are taken.

- Action**
1. Clear the firewall log on your router or switch.

```
user@myhost> clear firewall log
```

2. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **ssh *hostname*** command to verify that you can log in to the device using only SSH. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-A> ssh myhost
user@myhosts's password:
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC

% cli
user@myhost>
```

3. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **telnet *hostname*** command to verify that you can log in to your router or switch using only Telnet. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-A> telnet myhost
Trying 192.168.249.71...
Connected to myhost-fxp0.acme.net.
Escape character is '^['.
```

```
host (ttyp0)
```

```
login: user
```

Password:

```
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
```

```
% cli
user@myhost>
```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

```
user@myhost> show firewall log
```

Verifying Logged and Rejected Packets

Purpose Verify that the actions of the firewall filter terms are taken.

- Action** 1. Clear the firewall log on your router or switch.

```
user@myhost> clear firewall log
```

2. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **ssh hostname** command to verify that you cannot log in to the device using only SSH. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-B ssh myhost
ssh: connect to host sugar port 22: Connection refused
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
%
```

3. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **telnet hostname** command to verify that you can log in to the device using only Telnet. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the PFE.

```
user@host-B> telnet myhost
Trying 192.168.249.71...
telnet: connect to address 192.168.187.3: Connection refused
telnet: Unable to connect to remote host
%
```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

```
user@myhost> show firewall log
```

Time	Filter	Action	Interface	Protocol	Src Addr	Dest Addr
18:41:25	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
18:41:25	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
18:41:25	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
...						
18:43:06	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
18:43:06	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
18:43:06	local_acl	R	fxp0.0	TCP	192.168.187.5	192.168.187.1
...						

Related Documentation • [Example: Controlling Management Access on SRX Series Devices on page 1054](#)

The telnet Command

You can use the CLI **telnet** command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name>
<no-resolve> <port port> <routing-instance routing-instance-name> <source address>
```



NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent Telnet sessions is as follows:

SRX300	SRX320	SRX340	SRX345	SRX1500
3	3	3	5	5

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter **quit**.

Table 82 describes the **telnet** command options.

Table 82: CLI telnet Command Options

Option	Description
8bit	Use an 8-bit data path.
bypass-routing	Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open a Telnet session to the specified hostname or IP address.
inet	Force the Telnet session to an IPv4 destination.
interface source-interface	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
no-resolve	Suppress the display of symbolic names.
port port	Specify the port number or service name on the host.
routing-instance routing-instance-name	Use the specified routing instance for the Telnet session.
source address	Use the specified source address for the Telnet session.

- Related Documentation**
- [The ssh Command on page 1063](#)
 - [Configuring Password Retry Limits for Telnet and SSH Access on page 1052](#)
 - [Configuring Reverse Telnet and Reverse SSH on page 1053](#)

The ssh Command

You can use the CLI **ssh** command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name>  
<routing-instance routing-instance-name> <source address> <v1> <v2>
```



NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent SSH sessions is as follows:

SRX300	SRX320	SRX340	SRX345	SRX1500
3	3	3	5	5

Table 83 describes the **ssh** command options.

Table 83: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.
interface source-interface	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
routing-instance routing-instance-name	Use the specified routing instance for the SSH connection.
source address	Use the specified source address for the SSH connection.
v1	Force SSH to use version 1 for the connection.
v2	Force SSH to use version 2 for the connection.

- Related Documentation
- [The telnet Command on page 1062](#)
 - [Configuring Password Retry Limits for Telnet and SSH Access on page 1052](#)
 - [Configuring Reverse Telnet and Reverse SSH on page 1053](#)

Configuring Outbound SSH Service

You can configure a device running the Junos OS to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate the connection (for example, if the device is behind a firewall). The **outbound-ssh** command instructs the device to create a TCP/IP connection with the client management application and to forward the identity of the device. Once the connection is established, the management application acts as the client and initiates the SSH sequence, and the device acts as the server and authenticates the client.



NOTE: There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the device begins to initiate an outbound SSH connection based on the committed configuration. The device repeatedly attempts to create this connection until successful. If the connection between the device and the client management application is dropped, the device again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the device for outbound SSH connections, include the **outbound-ssh** statement at the **[edit system services]** hierarchy level:

[edit system services outbound-ssh]

The following topics describe the tasks for configuring the outbound SSH service:

- [Configuring the Device Identifier for Outbound SSH Connections on page 1064](#)
- [Sending the Public SSH Host Key to the Outbound SSH Client on page 1065](#)
- [Configuring Keepalive Messages for Outbound SSH Connections on page 1066](#)
- [Configuring a New Outbound SSH Connection on page 1066](#)
- [Configuring the Outbound SSH Client to Accept NETCONF as an Available Service on page 1066](#)
- [Configuring Outbound SSH Clients on page 1067](#)

Configuring the Device Identifier for Outbound SSH Connections

Each time the device establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the device to the management client. Within this transmission is the value of **device-id**.

To configure the device identifier of the device, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]  
device-id device-id;
```

The initiation sequence when **secret** is not configured:


```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

Sending the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

During the initialization of an SSH connection, the client authenticates the identity of the device using the public SSH host key of the device. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the device. When you configure the **secret** statement, the device passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the device establishes an outbound SSH connection, the device communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the **secret** statement. The value of the **secret** statement is shared between the device and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the device identified by the **device-id** statement.

Using the **secret** statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.



NOTE: Including the **secret** statement means that the device sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that device. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router's or switch's public SSH host key when the device connects to the client, include the **secret** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
secret password;
```

The following message is sent by the device when the **secret** attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-hot-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router's or switch's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the device using its copy of the router's or switch's public host SSH key as part of that sequence. The device authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the device to send SSH protocol keepalive messages to the client application, configure the **keep-alive** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
  retry number;
  timeout seconds;
}
```

Configuring a New Outbound SSH Connection

When disconnected, the device begins to initiate a new outbound SSH connection. To specify how the device reconnects to the server after a connection is dropped, include the **reconnect-strategy** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See [“Configuring Keepalive Messages for Outbound SSH Connections”](#) on page 1066.

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

To configure the application to accept NETCONF as an available service, include the **services netconf** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
  netconf;
}
```

Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]  
  address address {  
    retry number;  
    timeout seconds;  
    port port-number;  
  }
```



NOTE: Outbound SSH connections support IPv4 and IPv6 address formats.

PART 11

Configuring DNS

- [Configuring DNS Server Caching, DNSSEC, and DNS Proxy on page 1071](#)

CHAPTER 47

Configuring DNS Server Caching, DNSSEC, and DNS Proxy

- [DNS Overview on page 1071](#)
- [Example: Configuring the TTL Value for DNS Server Caching on page 1072](#)
- [DNSSEC Overview on page 1073](#)
- [Example: Configuring DNSSEC on page 1073](#)
- [Example: Configuring Keys for DNSSEC on page 1074](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 1074](#)
- [DNS Proxy Overview on page 1076](#)
- [Configuring the Device as a DNS Proxy on page 1080](#)

DNS Overview

A Domain Name System (DNS) is a distributed hierarchical system that converts hostnames to IP addresses. The DNS is divided into sections called zones. Each zone has name servers that respond to the queries belonging to their zones.

This topic includes the following sections:

- [DNS Components on page 1071](#)
- [DNS Server Caching on page 1072](#)

DNS Components

DNS includes three main components:

- **DNS resolver** — Resides on the client side of the DNS. When a user sends a hostname request, the resolver sends a DNS query request to the name servers to request the hostname's IP address.
- **Name servers** — Processes the DNS query requests received from the DNS resolver and returns the IP address to the resolver.
- **Resource records** — Data elements that define the basic structure and content of the DNS.

DNS Server Caching

DNS name servers are responsible for providing the hostname IP address to users. The TTL field in the resource record defines the period for which DNS query results are cached. When the TTL value expires, the name server sends a fresh DNS query and updates the cache.

- Related Documentation**
- [Example: Configuring the TTL Value for DNS Server Caching on page 1072](#)
 - [DNSSEC Overview on page 1073](#)

Example: Configuring the TTL Value for DNS Server Caching

This example shows how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

- [Requirements on page 1072](#)
- [Overview on page 1072](#)
- [Configuration on page 1072](#)
- [Verification on page 1073](#)

Requirements

No special configuration beyond device initialization is required before performing this task.

Overview

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

Configuration

Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds.

[edit]
user@host# **set system services dns max-cache-ttl 86400**
2. Specify the maximum TTL value for negative cached responses, in seconds.

[edit]
user@host# **set system services dns max-ncache-ttl 86400**
3. If you are done configuring the device, commit the configuration.

[edit]


```
user@host# commit
```

Verification

To verify the configuration is working properly, enter the **show system services** command.

Related Documentation

- [DNS Overview on page 1071](#)

DNSSEC Overview

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

Related Documentation

- [DNS Overview on page 1071](#)
- [Example: Configuring Keys for DNSSEC on page 1074](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 1074](#)

Example: Configuring DNSSEC

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]
```

```
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]
```

```
set system services dns dnssec disable
```

**Related
Documentation**

- [DNSSEC Overview on page 1073](#)

Example: Configuring Keys for DNSSEC

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key "...pasted-text..."
```

If you are done loading the keys from the file or terminal, click **commit** in the CLI editor.

**Related
Documentation**

- [DNSSEC Overview on page 1073](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 1074](#)

Example: Configuring Secure Domains and Trusted Keys for DNSSEC

This example shows how to configure secure domains and trusted keys for DNSSEC.

- [Requirements on page 1074](#)
- [Overview on page 1074](#)
- [Configuration on page 1075](#)

Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See [“Example: Configuring DNSSEC” on page 1073](#) for more information.

Overview

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.ABC123ABCh
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Step-by-Step Procedure To configure secure domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

```
[edit]
user@host# set system services dns dnssec secure-domains domain1.net
user@host# set system services dns dnssec secure-domains domain2.net
```

2. Configure trusted keys to domain1.net.

```
[edit]
user@host# set system services dns dnssec trusted-keys key
"domain1.net.ABC123ABCh"
```

3. Attach a root zone div.isc.org as a trusted anchor to a secure domain.

```
[edit]
user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor
dlv.isc.org
```

Results From configuration mode, confirm your configuration by entering the **show system services** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dns {
  dnssec {
    trusted-keys {
      key domain1.net.ABC123ABCh; ## SECRET-DATA
    }
    dlv {
      domain domain2.net trusted-anchor dlv.isc.org;
    }
    secure-domains {
      domain1.net;
      domain2.net;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

- Related Documentation**
- [DNSSEC Overview on page 1073](#)
 - [Example: Configuring Keys for DNSSEC on page 1074](#)

DNS Proxy Overview

A dynamic name system (DNS) proxy allows clients to use a device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

- [DNS Proxy Cache on page 1076](#)
- [DNS Proxy with Split DNS on page 1076](#)
- [Dynamic Domain Name System Client on page 1078](#)

DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.



NOTE: If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the **clear cache** command, or the cache will automatically expire along with TTL when it goes to zero.

DNS Proxy with Split DNS

The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

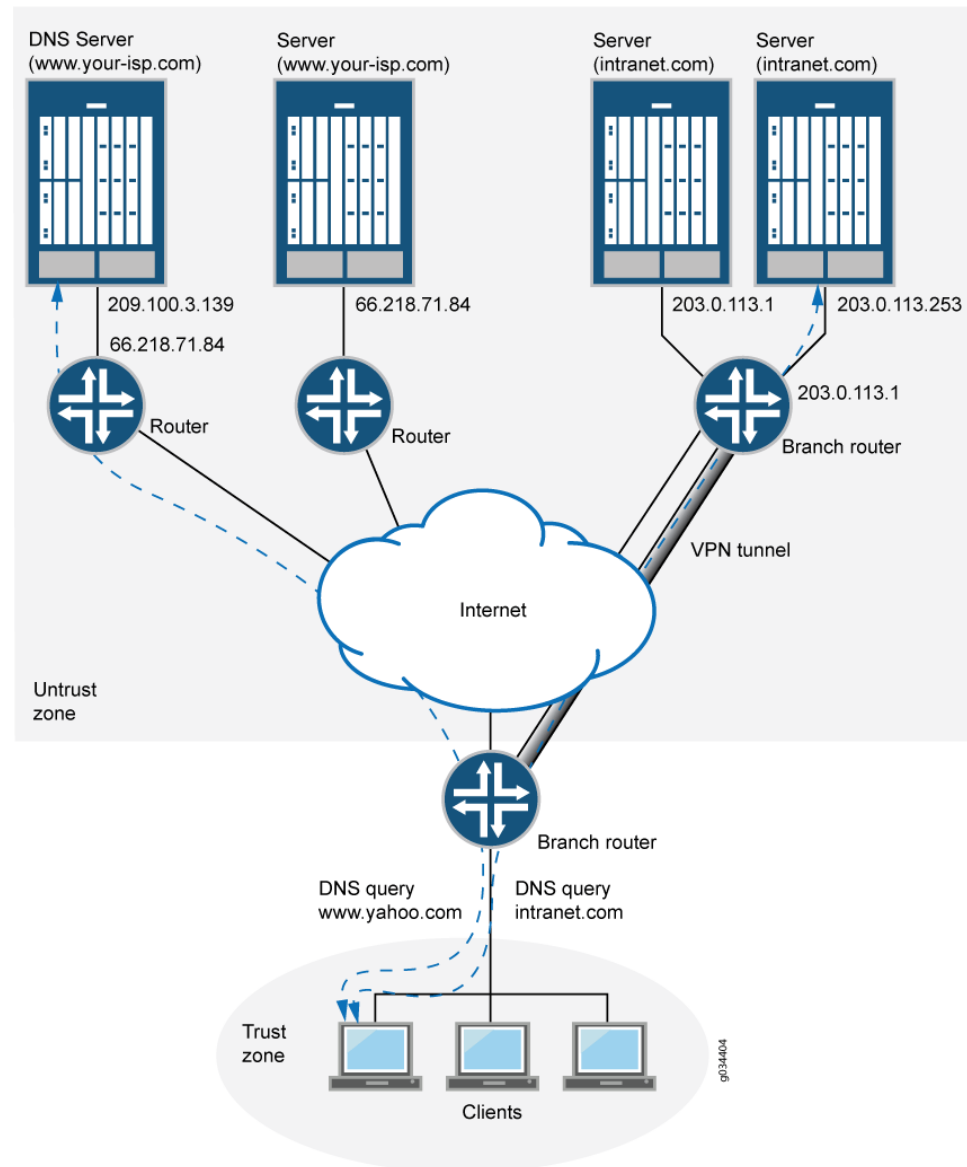
You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

Figure 31 shows how the split DNS proxy works in a corporate network.

Figure 31: DNS Proxy with Split DNS



In the corporate network shown in Figure 31, a PC client that points to the SRX Series device as its DNS server makes two queries—to `www.your-isp.com` and to `www.intranet.com`. The DNS proxy redirects the `www.intranet.com` query to the `www.intranet.com` DNS server (203.0.113.253), while the `www.your-isp.com` query is redirected to the ISP DNS server (209.100.3.130). Although the query for `www.your-isp.com` is sent to the ISP DNS server as a regular DNS query using clear text

protocols (TCP/UDP), the query for the `www.intranet.com` domain goes to the intranet's DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as `acme.com`) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.
- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

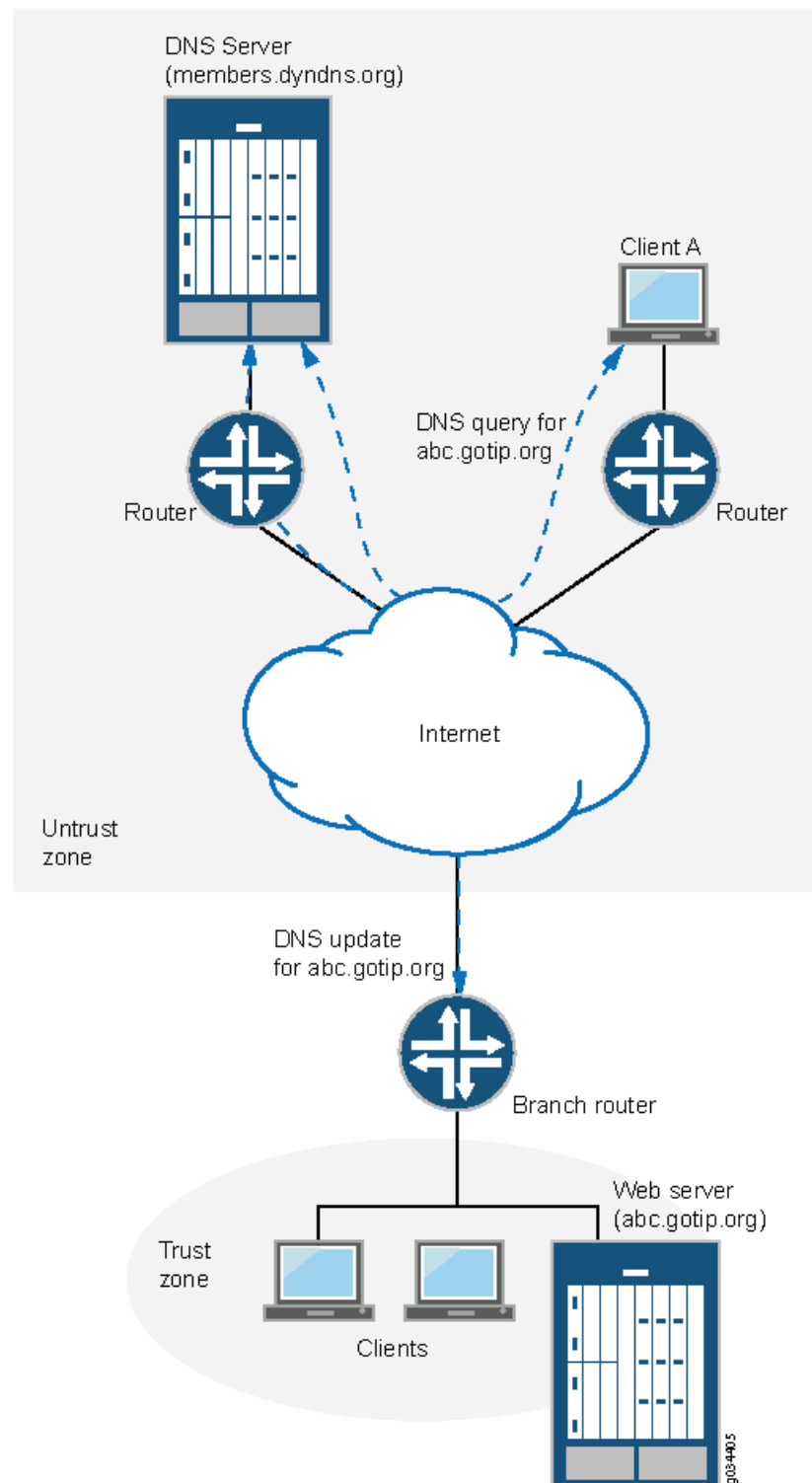
Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as `dyndns.org` and `ddo.jp`.

[Figure 32](#) illustrates how the DDNS client works.

Figure 32: Dynamic DNS



The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the untrust zone interface on the device. The hostname

abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in [Figure 32](#) needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

Related Documentation

- [Configuring the Device as a DNS Proxy on page 1080](#)

Configuring the Device as a DNS Proxy

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables a device to reference locations by domain name (such as www.example.net) in addition to using the routable IP address.

DNS features include:

- **DNS proxy**—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series device. DNS proxy improves domain lookup performance by using caching.
- **Split DNS**—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.
- **Dynamic DNS (DDNS) client**—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).

To configure the device as a DNS proxy, you enable DNS on a logical interface and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, ge-0/0/1.0—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

1. **DNS proxy configuration**
 - Enable DNS proxy on a logical interface.


```
[edit system services]
user@host# set dns dns-proxy interface ge-0/0/1.0
```

- Set a default domain name, and specify global name servers according to their IP addresses.

```
[edit system services]
user@host# set dns dns-proxy default-domain * forwarders 172.17.28.100
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns dns-proxy
```

2. Dynamic DNS proxy configuration

- Enable client.

```
[edit system services]
user@host# set dynamic-dns client abc.com agent juniper interface ge-0/0/1.0
username test password test123
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly

```
user@host# show system services dynamic-dns
```

Related Documentation

- [Configuring the Device as a DNS Proxy on page 1080](#)

PART 12

Configuring DHCP Access Service for IP Address Management

- [Understanding DHCP Services on page 1085](#)
- [Configuring a DHCP Local Server on page 1091](#)
- [Configuring a DHCP Client on page 1099](#)
- [Configuring a DHCP Relay Agent on page 1103](#)
- [Configuring a DHCPv6 Local Server on page 1107](#)
- [Configuring a DHCPv6 Client on page 1119](#)

Understanding DHCP Services

- [DHCP Overview on page 1085](#)
- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [DHCP Settings and Restrictions Overview on page 1089](#)

DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) can serve as a DHCP local server, a DHCP client, or a DHCP relay agent.

DHCP Local Server

You can enable an SRX Series device to function as a DHCP local server, and then configure its options on the device. The DHCP local server provides an IP address and other configuration information in response to a client request.

To configure the DHCP local server on the device, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level.



NOTE: You cannot configure the DHCP local server and the DHCP relay agent on the same interface.

DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the device. The following steps provide a high-level description of the interaction among the DHCP client, DHCP local server, and address-assignment pools.

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server and client installs the host route and ARP entry, and then monitors the lease state.

DHCP Local Server and Address-Assignment Pools

In a DHCP local server operation, the client address and configuration information reside in centralized address-assignment pools, that are managed independently from the DHCP local server and they can be shared by different client applications.

Configuring a DHCP environment that includes a DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the DHCP local server on the device and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.



NOTE: The DHCP local server and the address-assignment pools used by the server must be configured in the same routing instance.

DHCP Client

DHCP configuration consists of configuring DHCP clients and a DHCP local server. A client configuration determines how clients send a message requesting an IP address, while a server configuration enables the server to send an IP address back to the client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval.

DHCP Relay Agent

You can configure DHCP relay options on the device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP local server.

To configure the DHCP relay agent on the router, include the **dhcp-relay** statement at the **[edit forwarding-options]** hierarchy level.

You can also include the **dhcp-relay** statement at the following hierarchy level:

[edit routing-instances routing-instance-name forwarding-options]

DHCP Client, DHCP Relay Agent, and DHCP Local Servers

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the device between the DHCP client and one or more DHCP local servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP local server interact in a configuration that includes two DHCP local servers.

1. The DHCP client sends a discover packet to find a DHCP local server in the network from which to obtain configuration parameters for the subscriber, including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP local servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP local server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP local server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP local server from which to obtain configuration information.
6. The DHCP local server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
7. The DHCP relay agent receives the ACK packet and forwards it to the client.
8. The DHCP client receives the ACK packet and stores the configuration information.
9. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
10. After establishing the initial lease on the IP address, the DHCP client and the DHCP local server use unicast transmission to negotiate lease renewal or release.

Considerations

The following considerations apply when you enable a DHCP local server, DHCP relay agent, or DHCP client in a routing instance:

- The DHCP local server, DHCP relay agent, and DHCP client can be configured in one routing instance, but the functionality is mutually exclusive on one interface. If the DHCP client is enabled on one interface, the DHCP local server or the DHCP relay agent cannot be enabled on that interface.
- The DHCP client, DHCP relay agent and DHCP local server services act independently in their respective routing instance. The following features can function simultaneously on a device:

- DHCP client and DHCP local server
- DHCP client and DHCP relay agent
- Multiple routing instances. Each instance can have a DHCP local server, DHCP relay agent, or DHCP client, or each routing instance can have a DHCP client and DHCP local server or a DHCP client and DHCP relay agent.



NOTE: Before you enable DHCP services in a routing instance, you must remove all the configuration related to DHCP services that does not include routing instance support. If you do not do this, the old default routing instance configuration will override the new routing instance configuration.



NOTE: On all SRX Series devices, logical systems and routing instances are not supported for a DHCP client in chassis cluster mode.

**Related
Documentation**

- [Understanding DHCP Server Operation on page 1091](#)
- [Understanding DHCP Client Operation on page 1099](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)

DHCP Server, Client, and Relay Agent Overview

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network. An IP address can be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.

The device can also operate as a DHCP client and DHCP relay agent.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.



NOTE: Although a Juniper Networks device can act as a DHCP server, a DHCP client, or DHCP relay agent at the same time, you cannot configure more than one DHCP role on a single interface.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.



NOTE: On all SRX Series devices, DHCPv4 is supported only in Layer 3 mode; the DHCP server and DHCP client are not supported in Layer 2 transparent mode.

Related Documentation

- [DHCP Server Configuration Overview on page 1092](#)
- [Understanding DHCP Server Operation on page 1091](#)
- [Understanding DHCP Client Operation on page 1099](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)
- [DHCP Settings and Restrictions Overview on page 1089](#)

DHCP Settings and Restrictions Overview

This section contains the following topics:

- [Propagation of TCP/IP Settings for DHCP on page 1089](#)
- [DHCP Conflict Detection and Resolution on page 1089](#)
- [DHCP Interface Restrictions on page 1090](#)

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP's DHCP name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device's internal network.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the **show system services dhcp conflict** command. The addresses in the conflicts list remain excluded until you use the **clear system services dhcp conflict** command to manually clear the list.

DHCP Interface Restrictions

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types.

DHCP is not supported on interfaces that are part of a virtual private network (VPN).

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [Understanding DHCP Server Operation on page 1091](#)
- [Understanding DHCP Client Operation on page 1099](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)

CHAPTER 49

Configuring a DHCP Local Server

- [Understanding DHCP Server Operation on page 1091](#)
- [DHCP Server Configuration Overview on page 1092](#)
- [Minimum DHCP Local Server Configuration on page 1093](#)
- [Configuring Address-Assignment Pools on page 1094](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 1095](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 1095](#)
- [Configuring Static Address Assignments on page 1096](#)
- [Enabling TCP/IP Propagation on a DHCP Local Server on page 1096](#)
- [Verifying and Managing DHCP Local Server Configuration on page 1097](#)

Understanding DHCP Server Operation

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. Juniper Networks devices can also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

This section contains the following topics:

- [DHCP Options on page 1091](#)
- [Compatibility with Autoinstallation on page 1092](#)
- [Chassis Cluster Support on page 1092](#)

DHCP Options

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers

- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

Compatibility with Autoinstallation

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Chassis Cluster Support

DHCP server operations are supported on all SRX Series devices in chassis cluster mode.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [Understanding DHCP Client Operation on page 1099](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)

DHCP Server Configuration Overview

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device interface:

- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.
- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.
- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. [Table 84](#) provides the settings and values for the sample DHCP server configuration.

Table 84: Sample DHCP Server Configuration Settings

Setting	Sample Value
DHCP Subnet Configuration	
Address pool subnet address	192.168.2.0/24
High address in the pool range	192.168.2.254
Low address in the pool range	192.168.2.2

Table 84: Sample DHCP Server Configuration Settings (*continued*)

Setting	Sample Value
Address pool default lease time, in seconds	1,209,600 (14 days)
Address pool maximum lease time, in seconds	2,419,200 (28 days)
Domain search suffixes	mycompany.net mylab.net
Address to exclude from the pool	192.168.2.33
DNS server address	192.168.10.2
Identifier code for router solicitation address option	32
Type choice for router solicitation address option	ip address
IP address for router solicitation address option	192.168.2.33
DHCP MAC Address Configuration	
Static binding MAC address	01:03:05:07:09:0B
Fixed address	192.168.2.50

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [Understanding DHCP Server Operation on page 1091](#)
- [Understanding DHCP Client Operation on page 1099](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)
- [RFC 3397, Dynamic Host Configuration Protocol \(DHCP\) Domain Search Option](#)

Minimum DHCP Local Server Configuration

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP local server. In this output, the server group is named `mobileusers`, and the DHCP local server is enabled on interface `ge-1/0/1.0` within the group.

```
[edit access]
address-assignment {
  pool acmenetwork family inet {
    network 192.168.1.0/24;
  }
}

edit system services
dhcp-local-server {
```

```
group mobileusers {  
  interface ge-1/0/1.0  
}  
}  
  
edit interfaces ge-1/0/1 unit 0  
family {  
  inet {  
    address 192.168.1.1/24  
  }  
}
```



NOTE: You can configure the DHCP local server in a routing instance by using the `dhcp-local server`, `interface`, and `address-assignment` statements in the `[edit routing-instances]` hierarchy level.

Related Documentation

- [Configuring Address-Assignment Pools on page 1094](#)

Configuring Address-Assignment Pools

The address-assignment pool feature enables you to create address pools that can be shared by different client applications.

To configure an address-assignment pool:

1. Configure the address-assignment pool name and specify the addresses for the pool.
See [“Configuring an Address-Assignment Pool Name and Addresses” on page 1095](#).
2. (Optional) Configure named ranges (subsets) of addresses.
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 1095](#).
3. (Optional; IPv4 only) Create static address bindings.
See [“Configuring Static Address Assignments” on page 1096](#).
4. (Optional) Configure attributes for DHCP clients.
See [“Configuring DHCP Client-Specific Attributes for Address-Assignment Pools” on page 1100](#).

Related Documentation

- [Configuring an Address-Assignment Pool Name and Addresses on page 1095](#)

Configuring an Address-Assignment Pool Name and Addresses

When configuring an address-assignment pool, you must specify the name of the pool and its addresses.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the network address and the prefix length of the addresses in the pool.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set network 192.168.0.0/16
```



NOTE: You can configure an IPv4 address-assignment pool in a routing instance by configuring the address-assignment statements in the `[edit routing-instances]` hierarchy level.

Related Documentation

- [Configuring Address-Assignment Pools on page 1094](#)

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During a dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool isp_] family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```



NOTE: To configure named address ranges in a routing instance, configure the address-assignment statements in the `[edit routing-instances]` hierarchy level.

Related Documentation • [Configuring Address-Assignment Pools on page 1094](#)

Configuring Static Address Assignments

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address.

To configure a static IPv4 address binding:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 01:03:05:07:09:0b is always assigned IP address 192.168.10.2.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set host svale6_boston_net hardware-address 01:03:05:07:09:0b
ip-address 192.168.10.2
```



NOTE: To configure static binding for an IPv4 address in a routing instance, configure the address-assignment statements in the [edit routing-instances] hierarchy.

Related Documentation • [Configuring Address-Assignment Pools on page 1094](#)

Enabling TCP/IP Propagation on a DHCP Local Server

This topic describes how to configure TCP/IP settings on a DHCP local server, which includes a DHCP client and a DHCP local server.

To enable TCP/IP setting propagation on a DHCP local server:

1. Configure the **update-server** option on the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp-client {
  update-server;
}
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

```
[edit access]
address-assignment {
```



```

pool sprint family inet {
  network 192.168.2.0/24;
  dhcp-attributes {
    propagate-settings ge-0/0/1.0;
  }
}

```

3. Configure the DHCP local server.

```

edit system services
dhcp-local-server {
  group bob {
    interface ge-1/0/1.0
  }
}

```

Related Documentation

- [Minimum DHCP Local Server Configuration on page 1093](#)

Verifying and Managing DHCP Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the DHCP local server.

- Action**
- To display the address bindings in the client table on the DHCP local server:

```
user@host> show dhcp server binding
```

- To display DHCP local server statistics:

```
user@host> show dhcp server statistics
```

- To clear the binding state of a DHCP client from the client table on the DHCP local server:

```
user@host> clear dhcp server binding
```

- To clear all DHCP local server statistics:

```
user@host> clear dhcp server statistics
```



NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp server binding routing instance <routing-instance name>`
- `show dhcp server statistics routing instance <routing-instance name>`
- `clear dhcp server binding routing instance <routing-instance name>`
- `clear dhcp server statistics routing instance <routing-instance name>`

Related Documentation • [Minimum DHCP Local Server Configuration on page 1093](#)

Configuring a DHCP Client

- [Understanding DHCP Client Operation on page 1099](#)
- [Minimum DHCP Client Configuration on page 1099](#)
- [Configuring DHCP Client-Specific Attributes for Address-Assignment Pools on page 1100](#)
- [Configuring Optional DHCP Client Attributes on page 1101](#)
- [Verifying and Managing DHCP Client Configuration on page 1101](#)

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series devices in chassis cluster mode.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [Understanding DHCP Relay Agent Operation on page 1103](#)
- [DHCP Settings and Restrictions Overview on page 1089](#)

Minimum DHCP Client Configuration

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      dhcp-client
```

```

    }
  }
}

```



NOTE: To configure a DHCP client in a routing instance, add the interface in a routing instance using the [edit routing-instances] hierarchy.

Related Documentation

- [Configuring Optional DHCP Client Attributes on page 1101](#)

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot file that the client uses, the DNS server, and the maximum lease time.

You use the **dhcp-attributes** statement to configure DHCP client-specific attributes for address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name of the address-assignment pool.

```

[edit access]
user@host# edit address-assignment pool blr-pool family inet

```

2. Configure optional DHCP client attributes.

```

[edit access address-assignment pool blr-pool family inet]
user@host# set dhcp-attributes maximum-lease-time 2419200
user@host# set dhcp-attributes name-server 192.168.10.2
user@host# set dhcp-attributes boot-file boot-file.txt
user@host# set dhcp-attributes boot-file boot-server example.com

```



NOTE: To configure DHCP client-specific attributes in a routing instance, configure the **dhcp-attributes** statements in the [edit routing-instances] hierarchy.

Related Documentation

- [Configuring Address-Assignment Pools on page 1094](#)

Configuring Optional DHCP Client Attributes

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```



NOTE: To configure the DHCP client in a routing instance, configure the interface in the [edit routing-instances] hierarchy.

Related Documentation

- [Minimum DHCP Client Configuration on page 1099](#)

Verifying and Managing DHCP Client Configuration

Purpose View or clear information about client address bindings and statistics for the DHCP client.

- Action**
- To display the address bindings in the client table on the DHCP client:
`user@host> show dhcp client binding`
 - To display DHCP client statistics:
`user@host> show dhcp client statistics`
 - To clear the binding state of a DHCP client from the client table on the DHCP client:
`user@host> clear dhcp client binding`
 - To clear all DHCP client statistics:
`user@host> clear dhcp client statistics`



NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp client binding routing instance <routing-instance name>`
 - `show dhcp client statistics routing instance <routing-instance name>`
 - `clear dhcp client binding routing instance <routing-instance name>`
 - `clear dhcp client statistics routing instance <routing-instance name>`
-

Related •
Documentation

CHAPTER 51

Configuring a DHCP Relay Agent

- [Understanding DHCP Relay Agent Operation on page 1103](#)
- [Minimum DHCP Relay Agent Configuration on page 1104](#)
- [Verifying and Managing DHCP Relay Configuration on page 1104](#)

Understanding DHCP Relay Agent Operation

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.



NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [Understanding DHCP Server Operation on page 1091](#)
- [DHCP Settings and Restrictions Overview on page 1089](#)

Minimum DHCP Relay Agent Configuration

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP relay agent. In this output, the active server group is named server-1 and its IP address is 203.0.113.1. The DHCP relay agent configuration is applied to a group named bob. Within this group, the DHCP relay agent is enabled on interface ge-1/0/1.0.

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    server-1 {
      203.0.113.1;
    }
  }
  active-server-group server-1;
  group bob {
    interface ge-1/0/1.0;
  }
}
```



NOTE: To configure the DHCP relay agent in a routing instance, configure the `dhcp-relay` statements in the `[edit routing-instances]` hierarchy level.

Related Documentation

- [Verifying and Managing DHCP Relay Configuration on page 1104](#)

Verifying and Managing DHCP Relay Configuration

Purpose View or clear address bindings or statistics for DHCP relay agent clients.

Action • To display the address bindings for DHCP relay agent clients:

```
user@host> show dhcp relay binding
```

- To display DHCP relay agent statistics:

```
user@host> show dhcp relay statistics
```

- To clear the binding state of DHCP relay agent clients:

```
user@host> clear dhcp relay binding
```

- To clear all DHCP relay agent statistics:

```
user@host> clear dhcp relay statistics
```

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp relay binding routing instance <routing-instance name>`
- `show dhcp relay statistics routing instance <routing-instance name>`

- clear dhcp relay binding routing instance <routing-instance name>
- clear dhcp relay statistics routing instance <routing-instance name>



NOTE: On all SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

**Related
Documentation**

- [Minimum DHCP Relay Agent Configuration on page 1104](#)

Configuring a DHCPv6 Local Server

- [DHCPv6 Server Overview on page 1107](#)
- [Creating a Security Policy for DHCPv6 on page 1108](#)
- [Example: Configuring DHCPv6 Server Options on page 1109](#)
- [Example: Configuring an Address-Assignment Pool on page 1111](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 1114](#)
- [Configuring Address-Assignment Pool Linking on page 1114](#)
- [Configuring DHCP Client-Specific Attributes on page 1115](#)
- [Configuring an Address-Assignment Pool for Router Advertisement on page 1116](#)
- [Understanding DHCPv6 Client and Server Identification on page 1116](#)

DHCPv6 Server Overview

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IP version 6 (IPv6) clients and deliver configuration settings to client hosts on a subnet or to requesting devices that need an IPv6 prefix. A DHCPv6 server lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network.



NOTE: SRX Series devices do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)
- Prefix delegation, including access-internal route installation
- DHCPv6 server groups

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security

policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the **[edit system services dhcp-local-server]** hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the **[edit access address-assignment pool]** hierarchy level using the **family inet6** statement.

You can also include the **dhcpv6** statement at the **[edit routing-instances routing-instance-name system services dhcp-local-server]** hierarchy.



NOTE: Existing DHCPv4 configurations in the **[edit system services dhcp]** hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

Related Documentation

- [Example: Configuring DHCPv6 Server Options on page 1109](#)
- [Example: Configuring an Address-Assignment Pool on page 1111](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 1114](#)
- [Creating a Security Policy for DHCPv6 on page 1108](#)

Creating a Security Policy for DHCPv6

For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. In this example, the zone **my-zone** allows DHCPv6 traffic from the zone **untrust**, and the **ge-0/0/3.0** interface is configured with the IPv6 address **2001:db8:3001::1**.

To create a security zone policy to allow DHCPv6:

1. Create the zone and add an interface to that zone.

```
[edit security zones]
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```

2. Configure host inbound traffic system services to allow DHCPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]
user@host# set host-inbound-traffic system-services dhcpv6
```

3. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [DHCPv6 Server Overview on page 1107](#)
- [Example: Configuring DHCPv6 Server Options on page 1109](#)
- [Example: Configuring an Address-Assignment Pool on page 1111](#)

Example: Configuring DHCPv6 Server Options

This example shows how to configure DHCPv6 server options.

- [Requirements on page 1109](#)
- [Overview on page 1109](#)
- [Configuration on page 1109](#)
- [Verification on page 1111](#)

Requirements

Before you begin:

- Determine the IPv6 address pool range.
- Determine the IPv6 prefix. See the *Understanding Address Books*.
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients.
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.

Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the upto command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 2001:db8:3001::1/64 and set router advertisement for interface ge-0/0/3.0.



NOTE: A DHCPv6 group must contain at least one interface.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 upto
  ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides
  interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

```
[edit]  
user@host# edit system services dhcp-local-server dhcpv6
```
2. Set a default limit for all DHCPv6 groups.

```
[edit system services dhcp-local-server dhcpv6]  
user@host# set overrides interface-client-limit 100
```
3. Specify a group name and interface.

```
[edit system services dhcp-local-server dhcpv6]  
user@host# set group my-group interface ge-0/0/3.0
```
4. Set a range of interfaces.

```
[edit system services dhcp-local-server dhcpv6]  
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
```
5. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]  
user@host# set group my-group overrides interface-client-limit 200
```
6. Configure an interface with an IPv6 address.

```
[edit interfaces]  
user@host# set ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
```
7. Set router advertisement for the interface.

```
[edit protocols]  
user@host# set router-advertisement interface ge-0/0/3.0 prefix  
2001:db8:3000::/64
```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server**, **show interfaces ge-0/0/3**, and **show protocols** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]  
user@host# show system services dhcp-local-server  
dhcpv6 {  
  overrides {  
    interface-client-limit 100;  
  }  
  group my-group {  
    overrides {  
      interface-client-limit 200;  
    }  
    interface ge-0/0/3.0 {  
      upto ge-0/0/6.0;  
    }  
  }  
}
```

```

}
}
[edit]
user@host# show interfaces ge-0/0/3
unit 0 {
family inet6 {
address 2001:db8:3000::1/64;
}
}
[edit]
user@host# show protocols
router-advertisement {
interface ge-0/0/3.0 {
prefix 2001:db8:3000::1/64;
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying DHCPv6 Local Server Configuration

Purpose	Verify that the client address bindings and statistics for the DHCPv6 local server have been configured
Action	<p>From operational mode, enter these commands:</p> <ul style="list-style-type: none"> • show dhcpv6 server binding command to display the address bindings in the client table on the DHCPv6 local server. • show dhcpv6 server statistics command to display the DHCPv6 local server statistics. • clear dhcpv6 server bindings all command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance. • clear dhcpv6 server statistics command to clear all DHCPv6 local server statistics.
Related Documentation	<ul style="list-style-type: none"> • DHCPv6 Server Overview on page 1107 • Example: Configuring an Address-Assignment Pool on page 1111 • Configuring a Named Address Range for Dynamic Address Assignment on page 1114 • Creating a Security Policy for DHCPv6 on page 1108

Example: Configuring an Address-Assignment Pool

This example shows how to configure an address-assignment pool.

- [Requirements on page 1112](#)
- [Overview on page 1112](#)

- [Configuration on page 1112](#)
- [Verification on page 1113](#)

Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool.
- Set DHCPv6 attributes for the address-assignment pool.

Overview

In this example, you configure an address-pool called `my-pool` and specify the IPv6 family as `inet6`. You configure the IPv6 prefix as `2001:db8:3000:1::/64`, the range name as `range1`, and the IPv6 range for DHCPv6 clients from a low of `2001:db8:3000:1::/64` to a high of `2001:db8:3000:200::/64`. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as `2001:db8:3001::1`, the grace period as `3600`, and the maximum lease time as `120`.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low
  32001:db8:3000:1::/64 high 2001:db8:3000:200::/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
  2001:db8:3001::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period
  3600
set access address-assignment pool my-pool family inet6 dhcp-attributes
  maximum-lease-time 120
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool family inet6
```
2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set prefix 2001:db8:3000:1::/64
```



```
user@host# set range range1 low 2001:db8:3000:1::/64 high
2001:db8:3000:200::/64
```

3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:3001::1
```

4. Configure the DHCPv6 attribute for the grace period.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600
```

5. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes maximum-lease-time 120
```

Results From configuration mode, confirm your configuration by entering the **show access address-assignment** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access address-assignment
pool my-pool {
  family inet6 {
    prefix 2001:db8:3000:1::/64;
    range range1 {
      low 2001:db8:3000:1::/64 ;
      high 2001:db8:3000:200::/64;
    }
    dhcp-attributes {
      maximum-lease-time 120;
      grace-period 3600;
      dns-server {
        2001:db8:3001::1;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Configuration

Purpose Verify that the address-assignment pool has been configured.

Action From operational mode, enter the **show access address-assignment** command.

Related Documentation

- [DHCPv6 Server Overview on page 1107](#)
- [Example: Configuring DHCPv6 Server Options on page 1109](#)

- [Configuring a Named Address Range for Dynamic Address Assignment on page 1114](#)
- [Creating a Security Policy for DHCPv6 on page 1108](#)

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool2 family inet6
```

2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 2001:db8:3000:5::/64
user@host# set range range2 low 2001:db8:3000:2::/64 high 2001:db8:3000:300::/64
```

3. Configure DHCPv6 attributes for the address pool.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600
maximum-lease-time 120
```

4. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [Configuring Address-Assignment Pool Linking on page 1114](#)

Configuring Address-Assignment Pool Linking

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example, you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the device switches to pool B for addresses. When pool B is exhausted, the device switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool.

To link a primary address-assignment pool named `pool1` to a secondary pool named `pool2`:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```

**Related
Documentation**

- [Configuring a Named Address Range for Dynamic Address Assignment on page 1095](#)

Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

You use the **dhcp-attributes** statement to configure DHCPv6 client-specific attributes for address-assignment pools at the **[edit access address-assignment pool *pool-name* family inet6]** hierarchy.

[Table 85](#) describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 85: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
dns-server	IPv6 address of DNS server to which clients can send DNS queries	23
grace-period	Grace period offered with the lease	—
maximum-lease-time	Maximum lease time allowed by the DHCPv6 server	—
option	User-defined options	—
sip-server-address	IPv6 address of SIP outbound proxy server	22
sip-server-domain-name	Domain name of the SIP outbound proxy server	21

**Related
Documentation**

- [Configuring a Named Address Range for Dynamic Address Assignment on page 1114](#)

Configuring an Address-Assignment Pool for Router Advertisement

You can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:

1. Create the IPv6 address-assignment pool.
2. Specify that the address-assignment pool is used for router advertisement.

```
[edit access address-assignment]
user@host# set neighbor-discovery-router-advertisement router1
```

3. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [Configuring a Named Address Range for Dynamic Address Assignment on page 1114](#)

Understanding DHCPv6 Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or server. DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-llt)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Layer address (duid-ll)

The duid-llt DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

Related Documentation

- [DHCPv6 Client Overview on page 1120](#)

CHAPTER 53

Configuring a DHCPv6 Client

- [DHCPv6 Client Overview on page 1120](#)
- [Minimum DHCPv6 Client Configuration on page 1121](#)
- [Configuring Optional DHCPv6 Client Attributes on page 1122](#)
- [Configuring Nontemporary Address Assignment on page 1123](#)
- [Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation on page 1124](#)
- [Configuring Auto-Prefix Delegation on page 1124](#)
- [Configuring the DHCPv6 Client Rapid Commit Option on page 1125](#)
- [Configuring a DHCPv6 Client in Autoconfig Mode on page 1126](#)
- [Configuring TCP/IP Propagation on a DHCPv6 Client on page 1126](#)

DHCPv6 Client Overview

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the **dhcpv6-client** statement at the **[edit interfaces]** hierarchy level.



NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the **[edit routing-instances]** hierarchy.



NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.



NOTE: On all branch SRX Series devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 1121](#)

Minimum DHCPv6 Client Configuration

This topic describes the minimum configuration you must use to configure an SRX Series device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the DHCPv6 client type. The client type can be **autoconfig** or **statefull**.

- To enable DHCPv6 auto configuration mode, configure the client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

- For stateful address assignment, configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the identity association type.

- To configure identity association for nontemporary address (IA_NA) assignment, specify the **client-ia type** as **ia-na**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

- To configure identity association for prefix delegation (IA_PD), specify the **client-ia-type** as **ia-pd**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:

- Link Layer address (duid-ll)
- Link Layer address plus time (duid-llt)
- Vendor-assigned unique ID based on enterprise number (vendor)

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```



NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the `[edit routing-instances]` hierarchy.

Related Documentation

- [DHCPv6 Client Overview on page 1120](#)

Configuring Optional DHCPv6 Client Attributes

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:

- dns-server
- domain
- ntp-server
- sip-domain
- sip-server

For example, to specify the DHCPv6 client requested option as **dns-server**:

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set req-option dns-server
```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set retransmission-attempt 6
```

3. Configure the **update-server** option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

4. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

5. Configure the two-message (rapid commit) exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```



NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [edit routing-instances] hierarchy.



NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.



NOTE: On all branch SRX Series devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Related Documentation • [Minimum DHCPv6 Client Configuration on page 1121](#)

Configuring Nontemporary Address Assignment

Nontemporary address assignment is also known as stateful address assignment. In the stateful address assignment mode, the DHCPv6 client requests global addresses from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the global addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

[edit]

```
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]

```
user@host# set client-type statefull
```

3. Specify the IA_NA assignment.

[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]

```
user@host# set client-ia-type ia-na
```

Related Documentation • [Minimum DHCPv6 Client Configuration on page 1121](#)

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation

The DHCPv6 client requests IPv6 addresses and prefixes from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the IPv6 addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure identity association for nontemporary addresses (IA_NA) and identity association for prefix delegation (IA_PD):

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

4. Specify the IA_PD.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 1121](#)

Configuring Auto-Prefix Delegation

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating router delegates IPv6 prefixes to a requesting router. The requesting router then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

To configure auto-prefix delegation:

1. Configure the DHCPv6 client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the identity association type as **ia-pd** for prefix delegation.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DUID type.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]  
user@host# set client-identifier duid-type duid-ll
```

5. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]  
user@host# set update-router-advertisement interface ge-0/0/0
```

**Related
Documentation**

- [Minimum DHCPv6 Client Configuration on page 1121](#)
- [Configuring Optional DHCPv6 Client Attributes on page 1122](#)

Configuring the DHCPv6 Client Rapid Commit Option

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option:

1. Specify the DHCPv6 client interface.

```
[edit]  
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]  
user@host# set rapid-commit
```

**Related
Documentation**

- [DHCPv6 Client Overview on page 1120](#)

Configuring a DHCPv6 Client in Autoconfig Mode

A DHCPv6 client configured in autoconfig mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in autoconfig mode:

1. Configure the DHCPv6 client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the interface on which to configure router advertisement.

```
[edit protocols router-advertisement]
user@host# set interface ge-0/0/1.0
```

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 1121](#)
- [Configuring Optional DHCPv6 Client Attributes on page 1122](#)

Configuring TCP/IP Propagation on a DHCPv6 Client

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the **update-server** option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
```

```
user@host# set update-server
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

```
[edit access]
```

```
user@host# set address-assignment pool 2 family inet6 dhcp-attributes  
propagate-settings ge-0/0/0
```

- Related Documentation**
- [DHCPv6 Client Overview on page 1120](#)
 - [Minimum DHCPv6 Client Configuration on page 1121](#)

PART 13

Managing System Files

- [Performing File Management Tasks on page 1131](#)

Performing File Management Tasks

- [File Management Overview on page 1131](#)
- [Decrypting Configuration Files on page 1132](#)
- [Encrypting Configuration Files on page 1132](#)
- [Modifying the Encryption Key on page 1134](#)
- [Cleaning Up Files in J-Web on page 1134](#)
- [Cleaning Up Files with the CLI on page 1135](#)
- [Deleting Files on page 1136](#)
- [Deleting the Backup Software Image on page 1137](#)
- [Downloading Files on page 1137](#)
- [Configuring RADIUS System Accounting on page 1138](#)
- [Managing Accounting Files on page 1141](#)

File Management Overview

You can use the J-Web user interface and the CLI to perform routine file management operations such as archiving log files and deleting unused log files, cleaning up temporary files and crash files, and downloading log files from the routing platform to your computer. You can also encrypt the configuration files with the CLI to prevent unauthorized users from viewing sensitive configuration information.

Before you perform any file management tasks, you must perform the initial device configuration described in the Getting Started Guide for your device.

Related Documentation

- [Cleaning Up Files in J-Web on page 1134](#)
- [Cleaning Up Files with the CLI on page 1135](#)
- [Managing Accounting Files on page 1141](#)
- [Encrypting Configuration Files on page 1132](#)
- [Decrypting Configuration Files on page 1132](#)

Decrypting Configuration Files

To disable the encryption of configuration files on a device and make them readable to all:

1. Enter operational mode in the CLI.
2. Verify your permission to decrypt configuration files on this device by entering the encryption key for the device.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
Verifying EEPROM stored encryption key:
```

3. At the second prompt, reenter the encryption key.
4. Enter configuration mode in the CLI.
5. Enable configuration file decryption.

```
[edit]
user@host# edit system
user@host# set no-encrypt-configuration-files
```

6. Begin the decryption process by committing the configuration.

```
[edit]
user@host# commit
commit complete
```

Related Documentation

- [Encrypting Configuration Files on page 1132](#)

Encrypting Configuration Files

To configure an encryption key in EEPROM and determine the encryption process, enter one of the **request system set-encryption-key** commands in operational mode described in [Table 86](#).



NOTE: The **request system set-encryption-key** command is not supported on high-end SRX Series devices; therefore, this task does not apply to such devices.

Table 86: request system set-encryption-key Commands

CLI Command	Description
request system set-encryption-key	Sets the encryption key and enables default configuration file encryption: <ul style="list-style-type: none"> • AES encryption for the Canada and U.S. version of Junos OS • DES encryption for the international version of Junos OS

Table 86: request system set-encryption-key Commands (*continued*)

CLI Command	Description
request system set-encryption-key algorithm des	Sets the encryption key and specifies configuration file encryption by DES.
request system set-encryption-key unique	<p>Sets the encryption key and enables default configuration file encryption with a unique encryption key that includes the chassis serial number of the device.</p> <p>Configuration files encrypted with the unique key can be decrypted only on the current device. You cannot copy such configuration files to another device and decrypt them.</p>
request system set-encryption-key des unique	Sets the encryption key and specifies configuration file encryption by DES with a unique encryption key.

To encrypt configuration files on a device:

1. Enter operational mode in the CLI.
2. Configure an encryption key in EEPROM and determine the encryption process; for example, enter the **request system set-encryption-key** command.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
```

3. At the prompt, enter the encryption key. The encryption key must have at least six characters.

```
Enter EEPROM stored encryption key:juniper1
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the encryption key.
5. Enter configuration mode in the CLI.
6. Enable configuration file encryption to take place.

```
[edit]
user@host# edit system
user@host# set encrypt-configuration-files
```

7. Begin the encryption process by committing the configuration.

```
[edit]
user@host# commit
commit complete
```

Related Documentation

- [Managing Accounting Files on page 1141](#)
- [Decrypting Configuration Files on page 1132](#)

Modifying the Encryption Key

When you modify the encryption key, the configuration files are decrypted and then reencrypted with the new encryption key.

To modify the encryption key:

1. Enter operational mode in the CLI.
2. Configure a new encryption key in EEPROM and determine the encryption process; for example, enter the **request system set-encryption-key** command.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
```

3. At the prompt, enter the new encryption key. The encryption key must have at least six characters.

```
Enter EEPROM stored encryption key:juniperone
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the new encryption key.

Related Documentation

- [Managing Accounting Files on page 1141](#)
- [Encrypting Configuration Files on page 1132](#)
- [Decrypting Configuration Files on page 1132](#)

Cleaning Up Files in J-Web

You can use the J-Web user interface to rotate log files and delete unnecessary files on the device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives all information in the current log files and creates fresh log files.
- Deletes log files in **/var/log**—Deletes any files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes any files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes any core files that the device has written during an error.
- Deletes all software images (*.tgz files) in **/var/sw/pkg**—Deletes any software images copied to this directory during software upgrades.

To rotate log files and delete unnecessary files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.

2. In the Clean Up Files section, click **Clean Up Files**. The device rotates log files and identifies the files that can be safely deleted.

The J-Web user interface displays the files that you can delete and the amount of space that will be freed on the file system.

3. Click one of the following buttons on the confirmation page:
 - To delete the files and return to the Files page, click **OK**.
 - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation

- [Managing Accounting Files on page 1141](#)
- [Encrypting Configuration Files on page 1132](#)
- [Decrypting Configuration Files on page 1132](#)
- [Cleaning Up Files with the CLI on page 1135](#)

Cleaning Up Files with the CLI

You can use the CLI **request system storage cleanup** command to rotate log files and delete unnecessary files on the device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives all information in the current log files, deletes old archives, and creates fresh log files.
- Deletes log files in **/var/log**—Deletes any files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes any files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes any core files that the device has written during an error.
- Deletes all software images (***.tgz** files) in **/var/sw/pkg**—Deletes any software images copied to this directory during software upgrades.

To rotate log files and delete unnecessary files with the CLI:

1. Enter operational mode in the CLI.
2. Rotate log files and identify the files that can be safely deleted.

```
user@host> request system storage cleanup
```

The device rotates log files and displays the files that you can delete.

3. Enter **yes** at the prompt to delete the files.



NOTE: You can issue the `request system storage cleanup dry-run` command to review the list of files that can be deleted with the `request system storage cleanup` command, without actually deleting the files.



NOTE:

On SRX Series devices, the `/var` hierarchy is hosted in a separate partition (instead of the root partition). If Junos OS installation fails as a result of insufficient space:

- Use the `request system storage cleanup` command to delete temporary files.
- Delete any user-created files in both the root partition and under the `/var` hierarchy.

Related Documentation

- [Cleaning Up Files in J-Web on page 1134](#)
- [Managing Accounting Files on page 1141](#)
- [Encrypting Configuration Files on page 1132](#)
- [Decrypting Configuration Files on page 1132](#)

Deleting Files

You can use the J-Web user interface to delete an individual file from the device. When you delete the file, it is permanently removed from the file system.



CAUTION: If you are unsure whether to delete a file from the device, we recommend using the **Cleanup Files** tool. This tool determines which files can be safely deleted from the file system.

To delete files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Download and Delete Files section, click one of the following file types:
 - **Log Files**—Lists the log files located in the `/var/log` directory on the device.
 - **Temporary Files**—Lists the temporary files located in the `/var/tmp` directory on the device.
 - **Old Junos OS**—Lists the software images in the (`*.tgz` files) in the `/var/sw/pkg` directory on the device.
 - **Crash (Core) Files**—Lists the core files located in the `/var/crash` directory on the device.

The J-Web user interface displays the files located in the directory.

3. Check the box next to each file you plan to delete.
4. Click **Delete**.

The J-Web user interface displays the files you can delete and the amount of space that will be freed on the file system.

5. Click one of the following buttons on the confirmation page:
 - To delete the files and return to the Files page, click **OK**.
 - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation

- [Managing Accounting Files on page 1141](#)

Deleting the Backup Software Image

Junos OS keeps a backup image of the software that was previously installed so that you can downgrade to that version of the software if necessary. You can use the J-Web user interface to delete this backup image. If you delete this image, you cannot downgrade to this particular version of the software.

To delete the backup software image:

1. In the J-Web user interface, select **Maintain>Files**.
2. Review the backup image information listed in the Delete Backup Junos Package section.
3. Click the **Delete backup Junos package** link to delete the backup image.
4. Click one of the following buttons on the confirmation page:
 - To delete the backup image and return to the Files page, click **OK**.
 - To cancel the deletion of the backup image and return to the Files page, click **Cancel**.

Related Documentation

- [Deleting Files on page 1136](#)

Downloading Files

You can use the J-Web user interface to download a copy of an individual file from the device. When you download a file, it is not deleted from the file system.

To download files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Download and Delete Files section, click one of the following file types:
 - **Log Files**—Lists the log files located in the **/var/log** directory on the device.
 - **Temporary Files**—Lists the temporary files located in the **/var/tmp** directory on the device.

- **Old Junos OS**—Lists the software images located in the (***.tgz** files) in the **/var/sw/pkg** directory on the device.
- **Crash (Core) Files**—Lists the core files located in the **/var/crash** directory on the device.

The J-Web user interface displays the files located in the directory.

3. Click **Download** to download an individual file.
4. Choose a location for the browser to save the file.

The file is downloaded.

**Related
Documentation**

- [Managing Accounting Files on page 1141](#)

Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

Tasks for configuring RADIUS system accounting are:

1. [Configuring Auditing of User Events on a RADIUS Server on page 1138](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 1139](#)
3. [Configuring RADIUS Server Accounting on page 1139](#)

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        secret password;
        source-address address;
        timeout seconds;
      }
    }
  }
}
```

Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the **server** statement at the **[edit system accounting destination radius]** hierarchy level:

```
server {
  server-address {
    accounting-port port-number;
    max-outstanding-requests value;
    port port-number;
    retry value;
    secret password;
    source-address address;
    timeout seconds;
  }
}
```

server-address specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.



NOTE: If no RADIUS servers are configured at the **[edit system accounting destination radius]** statement hierarchy level, the Junos OS uses the RADIUS servers configured at the **[edit system radius-server]** hierarchy level.

accounting-port *port-number* specifies the RADIUS server accounting port number.

The default port number is 1813.



NOTE: If you enable RADIUS accounting at the **[edit access profile *profile-name* accounting-order]** hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the **accounting-port** statement.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" ").

In the **source-address** statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address (in case if radius-server address is IPv4) or IPv6 address (in case if radius-server address is IPv6) configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

If you use the **enhanced-accounting** statement at the **[edit system radius-options]** hierarchy level, the RADIUS attributes such as access method, remote port, and access privileges can be audited. You can limit the number of attribute values to be displayed for auditing by using the **enhanced-avs-max <number>** statement at the **[edit system accounting]** hierarchy level.

```
[edit system radius-options]
enhanced-accounting;

[edit system accounting]
enhanced-avs-max <number>;
```

When a Juniper Networks router or switch is configured with RADIUS accounting, it sends **Accounting-Start** and **Accounting-Stop** messages to the RADIUS server. These messages contain information about user activities such as software logins, configuration changes, and interactive commands. This information is typically used for monitoring a network, collecting usage statistics, and ensuring that users are billed properly.

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting:

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        server {
          10.5.5.5 {
            accounting-port 3333;
            secret $ABC123;
            source-address 10.1.1.1;
            retry 3;
            timeout 3;
          }
          10.6.6.6 secret $ABC123;
          10.7.7.7 secret $ABC123;
        }
      }
    }
  }
}
```

```

    }
  }
}

```

Managing Accounting Files

If you configure your system to capture accounting data in log files, set the location for your accounting files to the DRAM.

The default location for accounting files is the **cfs/var/log** directory on the CompactFlash (CF) card. The **nonpersistent** option minimizes the read/write traffic to your CF card. We recommend that you use the **nonpersistent** option for all accounting files configured on your system.

To store accounting log files in DRAM instead of the CF card:

1. Enter configuration mode in the CLI.
2. Create an accounting data log file in DRAM and replace *filename* with the name of the file.

[edit]

user@host# **edit accounting-options file *filename***

3. Store accounting log files in the DRAM file.

[edit]

user@host# **set file *filename* nonpersistent**



CAUTION: If log files for accounting data are stored on DRAM, these files are lost when the device reboots. Therefore, we recommend that you back up these files periodically.

Related Documentation

- [Accounting Options Overview on page 1673](#)

PART 14

Working with Junos OS Licenses

- [Managing Junos OS Licenses on page 1145](#)

CHAPTER 55

Managing Junos OS Licenses

- [Junos OS Feature License Keys on page 1145](#)
- [Software Feature Licenses for SRX Series Devices on page 1147](#)
- [Displaying License Keys in J-Web on page 1152](#)
- [Downloading License Keys on page 1152](#)
- [Generating a License Key on page 1152](#)
- [Saving License Keys on page 1153](#)
- [Updating License Keys on page 1154](#)
- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)

Junos OS Feature License Keys

This section contains the following topics:

- [License Key Components on page 1145](#)
- [License Management Fields Summary on page 1146](#)

License Key Components

A license key consists of two parts:

- **License ID**—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- **License data**—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string **XXXXXXXXXX** is the license ID, and the trailing block of data is the license data:

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx  
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx  
          xxxxxx xxxxxx xxx
```

The license data defines the device ID for which the license is valid and the version of the license.

License Management Fields Summary

The Licenses page displays a summary of licensed features that are configured on the device and a list of licenses that are installed on the device. The information on the license management page is summarized in [Table 87](#).

Table 87: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	Name of the licensed feature: <ul style="list-style-type: none"> • Features—Software feature licenses. • All features—All-inclusive licenses
Licenses Used	Number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the device for the particular feature.
Licenses Needed	Number of licenses required for legal use of the feature. Usage is determined by the configuration on the device: If a feature is configured and the license for that feature is not installed, a single license is needed.
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	Valid —The installed license key is valid. Invalid —The installed license key is not valid.
Version	Numeric version number of the license key.
Group	If the license defines a group license, this field displays the group definition. If the license requires a group license, this field displays the required group definition. NOTE: Because group licenses are currently unsupported, this field is always blank.
Enabled Features	Name of the feature that is enabled with the particular license.
Expiry	Verify that the expiration information for the license is correct. For Junos OS, only permanent licenses are supported. If a license has expired, it is shown as invalid.

- Related Documentation**
- [Generating a License Key on page 1152](#)
 - [Updating License Keys on page 1154](#)
 - [Saving License Keys on page 1153](#)

- [Downloading License Keys on page 1152](#)

Software Feature Licenses for SRX Series Devices

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 32](#) describes the Junos OS features that require licenses.

Table 88: Junos OS Feature Licenses

Junos OS License Requirements			
Feature	SRX550M	SRX1500	SRX5000 line
Access Manager	X		
BGP Route Reflectors			
Dynamic VPN	X		
IDP Signature Update*	X	X	X
Application Signature Update (Application Identification)*	X		X
Juniper-Kaspersky Antivirus*	X		
Juniper-Sophos Antivirus*	X	X	X
Juniper-Sophos Antispam*	X	X	X
Juniper-Enhanced Web filtering*	X	X	X
Juniper-Websense Web filtering*	X		
Logical Systems			X
UTM	X	X	X

* Indicates support on high-memory devices only.

[Table 33](#) lists the licenses you can purchase for each SRX Series software feature. Each license allows you to run the specified advanced software features on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 89: Junos OS Feature License Model Number for SRX Series Devices

Licensed Software Feature	Supported Devices	Model Number
Application Security and IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-APPSEC-A-1
		SRX550-APPSEC-A-3
		SRX550-APPSEC-A-5
	SRX5400	SRX5400-APPSEC-1
		SRX5400-APPSEC-3
		SRX5400-APPSEC-5
	SRX5600	SRX5600-APPSEC-A-1
		SRX5600-APPSEC-A-3
		SRX5600-APPSEC-A-5
	SRX5800	SRX5800-APPSEC-A-1
		SRX5800-APPSEC-A-3
		SRX5800-APPSEC-A-5
IDP updates (1 year, 3 years, and 5 years)	SRX550	SRX550-IDP
		SRX550-IDP-3
		SRX550-IDP-5
IDP subscription (1 year and 3 years)	SRX1500	SRX1500-IPS-1
		SRX1500-IPS-3
	SRX5400, SRX5600, SRX5800	SRX5K-IDP
		SRX5K-IDP-3
		SRX5K-IDP-3-R
		SRX5K-IDP-R
Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-K-AV
		SRX550-K-AV-3
		SRX550-K-AV-5
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S-AV
		SRX550-S-AV-3
		SRX550-S-AV-5

Table 89: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antivirus updates (1 year)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX550	SRX550-S2-AS
		SRX550-S2-AS-3
		SRX550-S2-AS-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5400	SRX5400-S-AV-1
		SRX5400-S-AV-3
		SRX5400-S-AV-5
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX5600	SRX5600-S-AV-1
	SRX5800	SRX5800-S-AV-1
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX550	SRX550-W-EWF
		SRX550-W-EWF-3
		SRX550-W-EWF-5
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX5400	SRX5400-W-EWF-1
		SRX5400-W-EWF-3
		SRX5400-W-EWF-5
Juniper-Enhanced Web filtering (1 year)	SRX5600	SRX5600-W-EWF-1
	SRX5800	SRX5800-W-EWF-1
Enterprise Bundle—Kaspersky Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-SMB4-CS
		SRX550-SMB4-CS-3
		SRX550-SMB4-CS-5

Table 89: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX550	SRX550-S-SMB4- CS
		SRX550-S-SMB4- CS-3
		SRX550-S-SMB4- CS-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years)	SRX1500	SRX1500-CS-BUN-1
		SRX1500-CS-BUN-3
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX5400	SRX5400-CS-BUN-1
		SRX5400-CS-BUN-3
		SRX5400-CS-BUN-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year)	SRX5600	SRX5600-CS-BUN-1
	SRX5800	SRX5800-CS-BUN-1
Dynamic VPN Client (5, 10, and 25 simultaneous users)	SRX550	SRX-RAC-5-LTU
		SRX-RAC-10-LTU
		SRX-RAC-25-LTU
Dynamic VPN Service (5, 10, 25, and 50 simultaneous users)	SRX550	SRX-RAC-5-LTU
	SRX550	SRX-RAC-10-LTU
	SRX550	SRX-RAC-25-LTU
	SRX550	SRX-RAC-50-LTU
Dynamic VPN Service (100 and 150 simultaneous users)	SRX550	SRX-RAC-100-LTU
		SRX-RAC-150-LTU
Dynamic VPN Service (250 simultaneous users)	SRX550 <i>NOTE:</i> Requires Junos OS 11.2R3 or later	SRX-RAC-250-LTU
Dynamic VPN Service (500 simultaneous users)	SRX550 <i>NOTE:</i> Requires Junos OS 11.2R3 or later	SRX-RAC-500-LTU

Table 89: Junos OS Feature License Model Number for SRX Series Devices *(continued)*

Licensed Software Feature	Supported Devices	Model Number
Express Path License (formerly known as <i>services offloading</i>)	SRX5400, SRX5600, SRX5800	SRX5K-SVCS-OFFLOAD-RTU
NOTE: Prior to Junos OS Release 12.3X48-D10, Express Path was a licensed software feature. Starting with Junos OS Release 12.3X48-D10, the Express Path license is no longer required to enable this functionality. Your previously acquired Express Path license will not be effective anymore.		
Logical Systems License (incremental 1, 5, and 25 numbers)	SRX5400	SRX-5400-LSYS-1
		SRX-5400-LSYS-5
		SRX-5400-LSYS-25
	SRX5600	SRX-5600-LSYS-1
		SRX-5600-LSYS-5
		SRX-5600-LSYS-25
	SRX5800	SRX-5800-LSYS-1
		SRX-5800-LSYS-5
		SRX-5800-LSYS-25
Sky Advanced Threat protection (1 year, 3 years)	SRX1500	SRX1500-ATP-1
		SRX1500-ATP-3
Command and Control feeds (1 year, 3 years)	SRX1500	SPOT-CC-1500-1Y
		SPOT-CC-1500-3Y

- Related Documentation
- [License Enforcement on page 224](#)
 - [Junos OS Feature License Keys on page 1145](#)
 - [Working with License Keys for SRX Series Devices](#)

Displaying License Keys in J-Web

To display license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the device.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

Related Documentation

- [Junos OS Feature License Keys on page 1145](#)
- [Generating a License Key on page 1152](#)
- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)
- [Downloading License Keys on page 1152](#)

Downloading License Keys

To download license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the device to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written.

Related Documentation

- [Junos OS Feature License Keys on page 1145](#)
- [Generating a License Key on page 1152](#)
- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)

Generating a License Key

To generate a license key:

1. Gather the authorization code that you received when you purchased your license as well as your device serial number.
2. Go to the Juniper Networks licensing page at:

<https://www.juniper.net/lcrs/generateLicense.do>

3. Enter the device serial number and authorization code in the webpage and click **Generate**. Depending on the type of license you purchased, you will receive one of the following responses:

- License key—If you purchased a perpetual license, you will receive a license key from the licensing management system. You can enter this key directly into the system to activate the feature on your device.
- License key entitlement—If you purchased a subscription-based license, you will receive a license key entitlement from the licensing management system. You can use this entitlement to validate your license on the Juniper Networks licensing server and download the feature license from the server to your device.

**Related
Documentation**

- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)
- [Updating License Keys on page 1154](#)
- [Downloading License Keys on page 1152](#)

Saving License Keys

To save license keys installed on the device:

1. From operational mode, save the installed license keys to a file or URL.

```
user@host>request system license save filename | url
```

For example, the following command saves the installed license keys to a file named **license.config**:

```
request system license save ftp://user@host/license.conf
```

**Related
Documentation**

- [Junos OS Feature License Keys on page 1145](#)
- [Generating a License Key on page 1152](#)
- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)
- [Downloading License Keys on page 1152](#)

Updating License Keys

To update a license key from the device:

1. From operational mode, do one of the following tasks:

- Update the license keys automatically.

```
user@host> request system license update
```



NOTE: The `request system license update` command will always use the default Juniper license server <https://ae1.juniper.net>

You can only use this command to update subscription-based licenses (such as UTM).

- Update the trial license keys automatically.

```
user@host> request system license update trial
```

Related Documentation

- [Junos OS Feature License Keys on page 1145](#)
- [Generating a License Key on page 1152](#)
- [Example: Adding a New License Key on page 1154](#)
- [Example: Deleting a License Key on page 1157](#)
- [Downloading License Keys on page 1152](#)

Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 1154](#)
- [Overview on page 1154](#)
- [Configuration on page 1155](#)
- [Verification on page 1156](#)

Requirements

Before you begin, confirm that your Junos OS feature requires you to purchase, install, and manage a separate software license.

Overview

You can add a license key from a file or URL, from a terminal, or from the J-Web user interface. Use the ***filename*** option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.) Use the ***url*** to send a subscription-based license key entitlement (such as UTM) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

In this example, the file name is `bgp-reflection`.

Configuration

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

From operational mode, you can add a license key in either way:

- From a file or URL:

```
user@hostname> request system license add bgp-reflection
```
- From the terminal:

```
user@hostname> request system license add terminal
```

GUI Step-by-Step Procedure To add a new license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do one of the following, using a blank line to separate multiple license keys:
 - In the **License File URL** box, type the full URL to the destination file containing the license key to be added.
 - In the **License Key Text** box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure To add a new license key:

1. From operational mode, add a license key in either way:
 - From a file or URL:

```
user@host> request system license add bgp-reflection
```
 - From the terminal:

```
user@host>request system license add terminal
```
2. When prompted, enter the license key, separating multiple license keys with a blank line. If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.

Results From operational mode, confirm your configuration by entering the **show system license** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@hostname> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp-reflection	0	1	0	permanent

Licenses installed:

License identifier: G0300000xxxx

License version: 2

Valid for device: JN001875AB

Features:

bgp-reflection - Border Gateway Protocol route reflection
permanent

License identifier: G0300000xxxx

License version: 2

Valid for device: JN001875AB

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Installed Licenses

Purpose Verify that the expected licenses have been installed and are active on the device.

Action From operational mode, enter the **show system license** command.

The output shows a list of the licenses used and a list of the licenses installed on the device and when they expire.

Verifying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From operational mode, enter the **show system license usage** command.

```
user@hostname> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp-reflection	1	1	0	permanent

The output shows a list of the licenses installed on the device and how they are used.

Verifying Installed License Keys

Purpose Verify that the license keys were installed on the device.

Action From operational mode, enter the **show system license keys** command.

```
user@hostname> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
```

The output shows a list of the license keys installed on the device. Verify that each expected license key is present.

Related Documentation

- [Junos OS Feature License Keys on page 1145](#)
- [Generating a License Key on page 1152](#)
- [Example: Deleting a License Key on page 1157](#)
- [Updating License Keys on page 1154](#)
- [Downloading License Keys on page 1152](#)

Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 1157](#)
- [Overview on page 1157](#)
- [Configuration on page 1157](#)
- [Verification on page 1158](#)

Requirements

Before you delete a license key, confirm that it is no longer needed.

Overview

You can delete a license key from the CLI or J-Web user interface. In this example, the license ID is G0300000xxxx.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
user@host> request system license delete G0300000xxxx
```

GUI Step-by-Step Procedure

To delete a license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Select the check box of the license or licenses you want to delete.

3. Click **Delete**.
4. Click **OK** to check your configuration and save it as a candidate configuration.
5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To delete a license key:

1. From operational mode, for each license, enter the following command and specify the license ID. You can delete only one license at a time.

```
user@host> request system license delete G0300000xxxx
```

Results

From configuration mode, confirm your deletion by entering the **show system license** command. The license key you deleted will be removed. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying Installed Licenses on page 1158](#)

Verifying Installed Licenses

Purpose

Verify that the expected licenses have been removed from the device.

Action

From operational mode, enter the **show system license** command.

Related Documentation

- [Generating a License Key on page 1152](#)
- [Example: Adding a New License Key on page 1154](#)
- [Updating License Keys on page 1154](#)
- [Downloading License Keys on page 1152](#)

PART 15

Configuration Statements and Operational Commands

- [Configuration Statements on page 1161](#)
- [Operational Commands on page 1289](#)

CHAPTER 56

Configuration Statements

- [\[edit security certificates\] Hierarchy Level on page 1163](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 1164](#)
- [Groups Configuration Statement Hierarchy on page 1164](#)
- [System Configuration Statement Hierarchy on page 1165](#)
- [address-assignment \(Access\) on page 1196](#)
- [address-pool \(Access\) on page 1199](#)
- [allow-configuration on page 1200](#)
- [allow-configuration-regexps on page 1200](#)
- [authentication-key on page 1201](#)
- [authentication-order on page 1202](#)
- [boot-server \(NTP\) on page 1203](#)
- [broadcast on page 1204](#)
- [broadcast-client on page 1205](#)
- [ciphers on page 1206](#)
- [connection-limit on page 1207](#)
- [client-ia-type on page 1208](#)
- [client-identifier \(dhcp-client\) on page 1208](#)
- [client-identifier \(dhcpv6-client\) on page 1209](#)
- [client-list-name \(SNMP\) on page 1209](#)
- [client-type on page 1210](#)
- [deny-configuration on page 1210](#)
- [deny-configuration-regexps on page 1211](#)
- [destination \(Accounting\) on page 1212](#)
- [dhcp-attributes \(Access IPv4 Address Pools\) on page 1213](#)
- [dhcp-attributes \(Access IPv6 Address Pools\) on page 1215](#)
- [dhcp-client on page 1216](#)
- [dhcp-local-server \(System Services\) on page 1217](#)
- [dhcpv6 \(System Services\) on page 1221](#)

- [dhcpv6-client](#) on page 1224
- [disable \(System Services\)](#) on page 1225
- [dlv](#) on page 1225
- [family \(Security Forwarding Options\)](#) on page 1226
- [file \(System Logging\)](#) on page 1227
- [forwarding-options \(Security\)](#) on page 1230
- [group \(System Services DHCP\)](#) on page 1231
- [host \(SSH Known Hosts\)](#) on page 1234
- [hostkey-algorithm](#) on page 1235
- [interface \(System Services DHCP\)](#) on page 1236
- [interfaces \(ARP\)](#) on page 1237
- [interfaces \(Security Zones\)](#) on page 1238
- [interface-traceoptions \(System Services DHCP\)](#) on page 1239
- [internet-options](#) on page 1241
- [kernel-replication \(System\)](#) on page 1242
- [lease-time \(dhcp-client\)](#) on page 1242
- [location](#) on page 1243
- [lockout-period](#) on page 1244
- [macs](#) on page 1245
- [max-pre-authentication-packets](#) on page 1246
- [multicast-client](#) on page 1246
- [name-server \(Access\)](#) on page 1247
- [neighbor-discovery-router-advertisement \(Access\)](#) on page 1247
- [ntp](#) on page 1248
- [outbound-ssh](#) on page 1249
- [overrides \(System Services DHCP\)](#) on page 1251
- [peer \(NTP\)](#) on page 1252
- [prefix](#) on page 1253
- [proflerd](#) on page 1253
- [proxy](#) on page 1254
- [radius-options](#) on page 1255
- [radius-server](#) on page 1256
- [rapid-commit](#) on page 1257
- [reconfigure \(System Services DHCP\)](#) on page 1258
- [req-option](#) on page 1259
- [retransmission-attempt \(dhcp-client\)](#) on page 1260
- [retransmission-attempt \(dhcpv6-client\)](#) on page 1260

- [retransmission-interval \(dhcp-client\)](#) on page 1261
- [root-authentication](#) on page 1262
- [single-connection](#) on page 1263
- [server \(NTP\)](#) on page 1264
- [server-address \(dhcp-client\)](#) on page 1265
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\)](#) on page 1265
- [ssh-known-hosts](#) on page 1266
- [static-subscribers](#) on page 1267
- [statistics-service](#) on page 1267
- [subscriber-management](#) on page 1268
- [subscriber-management-helper](#) on page 1268
- [system master password](#) on page 1269
- [tacplus](#) on page 1270
- [tacplus-options](#) on page 1271
- [tacplus-server](#) on page 1272
- [traceoptions \(Outbound SSH\)](#) on page 1274
- [traceoptions \(System Services DHCP\)](#) on page 1276
- [trusted-key](#) on page 1278
- [uac-service](#) on page 1279
- [update-router-advertisement](#) on page 1280
- [update-server \(dhcp-client\)](#) on page 1280
- [update-server \(dhcpv6-client\)](#) on page 1280
- [usb-control](#) on page 1281
- [use-interface](#) on page 1281
- [user-id](#) on page 1282
- [vendor-id](#) on page 1282
- [vpn \(Forwarding Options\)](#) on page 1283
- [watchdog](#) on page 1283
- [web-management](#) on page 1284
- [web-management \(System Services\)](#) on page 1285

[edit security certificates] Hierarchy Level

```
security {  
  certificates {  
    cache-size bytes;  
    cache-timeout-negative seconds;  
    certification-authority profile-name {  
      ca-name name;  
      crl filename;  
      encoding (binary | pem);  
    }  
  }  
}
```

```
        enrollment-url url;  
        file filename;  
        ldap-url url;  
    }  
    enrollment-retry number;  
    local name {  
        certificate;  
        load-key-file url;  
    }  
    maximum-certificates number;  
    path-length length;  
}  
}
```

- Related Documentation**
- [Security Configuration Statement Hierarchy](#)
 - [Installation and Upgrade Guide](#)

[\[edit security ssh-known-hosts\] Hierarchy Level](#)

```
security {  
  ssh-known-hosts {  
    fetch-from-server server-name;  
    host hostname {  
      dsa-key dsa-key;  
      ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;  
      ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;  
      ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;  
      rsa-key rsa-key;  
      rsa1-key rsa1-key;  
    }  
    load-key-file key-file;  
  }  
}
```

- Related Documentation**
- [Security Configuration Statement Hierarchy](#)

[Groups Configuration Statement Hierarchy](#)

Use the statements in the **groups** configuration hierarchy to configure information that can be dynamically updated in various parts of the device configuration.

```
groups {  
  group-name {  
    configuration-data ;  
  }  
}
```

- Related Documentation**
- [Understanding Junos OS Configuration Groups on page 614](#)

System Configuration Statement Hierarchy

Use the statements in the **system** configuration hierarchy to configure system management functions including addresses of the Domain Name System (DNS) servers; device's hostname, address, and domain name; health monitoring; interface filtering; properties of the device's auxiliary and console ports; security profiles for logical systems; time zones and Network Time Protocol (NTP) properties; trace options; and user login accounts, including user authentication and the root-level user account. Statement descriptions that are exclusive to the SRX Series devices running Junos OS are described in this section.

```
system {
  accounting {
    destination {
      radius {
        server server-address {
          accounting-port port-number;
          max-outstanding-requests number;
          port number;
          retry number;
          secret password;
          source-address address;
          timeout seconds;
        }
      }
    }
    tacplus {
      server server-address {
        port port-number;
        secret password;
        single-connection;
        source-address source-address;
        timeout seconds;
      }
    }
  }
  events [change-log interactive-commands login];
  traceoptions {
    file {
      filename;
      files number;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
allow-v4mapped-packets;
archival {
  configuration {
    archive-sites url {
      password password;
    }
  }
}
```

```
        transfer-interval interval;  
        transfer-on-commit;  
    }  
}  
arp {  
    aging-timer minutes;  
    gratuitous-arp-delay seconds;  
    gratuitous-arp-on-ifup;  
    interfaces {  
        interface name {  
            aging-timer minutes;  
        }  
    }  
    passive-learning;  
    purging;  
}  
authentication-order [password radius tacplus];  
auto-configuration {  
    traceoptions {  
        file {  
            filename;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        level (all | error | info | notice | verbose | warning);  
        no-remote-trace;  
    }  
}  
auto-snapshot;  
autoinstallation {  
    configuration-servers {  
        url {  
            password password;  
        }  
    }  
    interfaces {  
        interface-name {  
            bootp;  
            rarp;  
        }  
    }  
    usb {  
        disable;  
    }  
}  
auto-snapshot;  
backup-router {  
    address;  
    destination [network];  
}  
commit {  
    server {  
        commit-interval seconds;
```

```

days-to-keep-error-logs days;
maximum-aggregate-pool number;
maximum entries number;
traceoptions {
  file {
    filename;
    files number;
    microsecond-stamp;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
synchronize;
}
compress-configuration-files;
default-address-selection;
diag-port-authentication {
  encrypted-password password;
  plain-text-password;
}
domain-name domain-name;
domain-search [domain-list];
donot-disable-ip6op-ondad;
dump-device (boot-device | compact-flash | usb);
dynamic-profile-options {
  versioning;
}
encrypt-configuration-files;
extensions {
  providers {
    provider-id {
      license-type license deployment-scope [deployments];
    }
  }
}
resource-limits {
  package package-name {
    resources {
      cpu {
        priority number;
        time seconds;
      }
      file {
        core-size bytes;
        open number;
        size bytes;
      }
      memory {
        data-size mbytes;
        locked-in mbytes;
        resident-set-size mbytes;
        socket-buffers mbytes;
        stack-size mbytes;
      }
    }
  }
}

```

```

    }
  }
  process process-ui-name {
    resources {
      cpu {
        priority number;
        time seconds;
      }
      file {
        core-size bytes;
        open number;
        size bytes;
      }
      memory {
        data-size mbytes;
        locked-in mbytes;
        resident-set-size mbytes;
        socket-buffers mbytes;
        stack-size mbytes;
      }
    }
  }
}
}
fips {
  level (0 | 1 | 2 | 3 | 4);
}
host-name hostname;
inet6-backup-router {
  address;
  destination destination;
}
internet-options {
  icmpv4-rate-limit {
    bucket-size seconds;
    packet-rate packets-per-second;
  }
  icmpv6-rate-limit {
    bucket-size seconds;
    packet-rate packets-per-second;
  }
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  ipv6-duplicate-addr-detection-transmits number;
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout minutes;
  no-tcp-reset (drop-all-tcp | drop-tcp-with-syn-only);
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit upper-limit;
  (source-quench | no-source-quench);
  tcp-drop-synfin-set;
  tcp-mss bytes;
}
kernel-replication;
license {

```



```

autoupdate {
  url url;
  password password;
}
renew {
  before-expiration number;
  interval interval-hours;
}
traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
location {
  altitude feet;
  building name;
  country-code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
login {
  announcement text;
  class class-name {
    access-end hh:mm;
    access-start hh:mm;
    allow-commands regular-expression;
    allow-configuration regular-expression;
    allow-configuration-regexps [regular-expression];
    allowed-days [day];
    deny-commands regular-expression;
    deny-configuration regular-expression;
    deny-configuration-regexps [regular-expression];
    idle-timeout minutes;
    logical-system logical-system;
    login-alarms;
    login-script script;
    login-tip;
    permissions [permissions ];
    security-role (audit-administrator | crypto-administrator | ids-administrator |
      security-administrator);
  }
  deny-sources {

```

```
    address [address-or-hostname];
  }
  message text;
}
password {
  change-type (character-set | set-transitions);
  format (des | md5 | sha1);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
}
retry-options {
  backoff-factor seconds;
  backoff-threshold number;
  lockout-period time;
  maximum-time seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}
user username {
  authentication {
    encrypted-password password;
    load-key-file url;
    plain-text-password;
    ssh-dsa public-key;
    ssh-rsa public-key;
  }
  class class-name;
  full-name complete-name;
  uid uid-value;
}
}
log-vital {
  interval minutes;
  files days;
  storage-limit percentage;
  file-size Mbytes;
  add oid{
    comment comment;
  }
  group {
    operating;
    idp;
    storage;
    cluster-counter;
    screen zone-name;
    spu spu-name;
  }
}
max-configuration-rollback number;
max-configurations-on-flash number;
mirror-flash-on-disk;
name-server ip-address;
nd-maxmcast-solicit value;
nd-retransmit-timer value;
no-compress-configuration-files;
```

```

no-debugger-on-alt-break;
no-multicast-echo;
no-neighbor-learn;
no-ping-record-route;
no-ping-time-stamp;
no-redirects;
no-saved-core-context;
ntp {
    authentication-key key-number {
        type md5;
        value password;
    }
    boot-server address;
    broadcast broadcast-address {
        key key;
        ttl value;
        version version;
    }
    broadcast-client;
    multicast-client {
        address;
    }
    peer peer-address {
        key key;
        prefer;
        version version;
    }
    server server-address {
        key key;
        prefer;
        version version;
    }
    source-address source-address;
    trusted-key [key-number];
}
pic-console-authentication {
    encrypted-password password;
    plain-text-password;
}
ports {
    auxiliary {
        disable;
        insecure;
        type (ansi | small-xterm | vt100 | xterm);
    }
    console {
        disable;
        insecure;
        log-out-on-disconnect;
        type (ansi | small-xterm | vt100 | xterm);
    }
}
processes {
    802.1x-protocol-daemon {
        command binary-file-path;
        disable;
    }
}

```

```
}
adaptive-services {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
alarm-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
application-identification {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
application-security {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
audit-process {
    command binary-file-path;
    disable;
}
auto-configuration {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
bootp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
chassis-control {
    disable;
    failover alternate-media;
}
class-of-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
craft-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
database-replication {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
datapath-trace-service {
    disable;
}
```

```

traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
dhcp {
  command binary-file-path;
  disable;
}
dhcp-service {
  disable;
  failover (alternate-media | other-routing-engine);
  interface-traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
}
dialer-services {
  disable;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
  }
  flag flag;
}

```

```
        no-remote-trace;
    }
}
diameter-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
disk-monitoring {
    command binary-file-path;
    disable;
}
dynamic-flow-capture {
    command binary-file-path;
    disable;
}
ecc-error-logging {
    command binary-file-path;
    disable;
}
ethernet-connectivity-fault-management {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ethernet-link-fault-management {
    command binary-file-path;
    disable;
}
ethernet-switching {
    command binary-file-path;
    disable;
}
event-processing {
    command binary-file-path;
    disable;
}
fipsd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

```

}
firewall-authentication-service {
    disable;
}
forwarding {
    command binary-file-path;
    disable;
}
general-authentication-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
gprs-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
group-key-member {
    disable;
}
group-key-server {
    disable;
}
idp-policy {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ilmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
inet-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
init {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
interface-control {
    command binary-file-path;
    disable;
}

```

```
    failover (alternate-media | other-routing-engine);
}
ipmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ipsec-key-management {
    (disable | enable);
}
jsrp-service {
    disable;
}
jtasktest {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
kernel-replication {
    command binary-file-path;
    disable;
}
l2-learning {
    command binary-file-path;
    disable;
}
l2cpd-service {
    command binary-file-path;
    disable;
}
lACP {
    command binary-file-path;
    disable;
}
lldpd-service {
    command binary-file-path;
    disable;
}
logical-system-mux {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
logical-system-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
```



```
}
mib-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mobile-ip {
    command binary-file-path;
    disable;
}
mountd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mspd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
multicast-snooping {
    command binary-file-path;
    disable;
}
named-service {
    disable;
    failover (alternate-media | other-routing-engine);
}
neighbor-liveness {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
network-security {
    disable;
}
network-security-trace {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
nfsd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ntp {
    disable;
    failover (alternate-media | other-routing-engine);
}
ntpd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
peer-selection-service {
```

```
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
periodic-packet-services {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pgcp-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pgm {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
pic-services-logging {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
ppp {  
    command binary-file-path;  
    disable;  
}  
pppoe {  
    command binary-file-path;  
    disable;  
}  
process-monitor {  
    disable;  
    traceoptions {  
        file {  
            filename;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        level (all | error | info | notice | verbose | warning);  
        no-remote-trace;  
    }  
}  
profilerd {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
r2cp {  
    command binary-file-path;  
    disable;  
}
```

```

redundancy-interface-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
remote-operations {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
resource-cleanup {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
routing {
    disable;
    failover (alternate-media | other-routing-engine);
}
sampling {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
sbc-configuration-process {
    disable;
    failover (alternate-media | other-routing-engine);
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
sdk-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;

```

```
        size maximum-file-size;  
        (world-readable | no-world-readable);  
    }  
    flag flag;  
    level (all | error | info | notice | verbose | warning);  
    no-remote-trace;  
}  
}  
secure-neighbor-discovery {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
security-log {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
send {  
    disable;  
}  
service-deployment {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
shm-rtssdbd {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
simple-mail-client-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
smtpd-service {  
    disable;  
}  
snmp {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
static-subscribers {  
    disable;  
}  
statistics-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}  
subscriber-management {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);
```

```

}
subscriber-management-helper {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
system-health-management {
    disable;
}
system-log-vital {
    disable;
}
tunnel-oamd {
    command binary-file-path;
    disable;
}
uac-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
usb-control {
    command binary-file-path;
    disable;
}
virtualization-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
wan-acceleration {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
watchdog {
    enable;
    disable;
    timeout value;
}
web-management {
    disable;
}

```

```
    failover (alternate media | other-routing-engine);
  }
  wireless-lan-service {
    disable;
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
  wireless-wan-service {
    disable;
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
  proxy {
    password password;
    port port-number;
    server url;
    username user-name;
  }
  radius-options {
    attributes {
      nas-ip-address nas-ip-address;
    }
    password-protocol mschap-v2;
  }
  radius-server server-address {
    accounting-port number;
    max-outstanding-requests number;
    port number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
  }
  root-authentication {
    encrypted-password password;
    load-key-file url;
    plain-text-password;
    ssh-dsa public-key {
```

```

    <from pattern-list>;
  }
  ssh-rsa public-key {
    <from pattern-list>;
  }
}
saved-core-context;
saved-core-files number;
scripts {
  commit {
    allow-transients;
    direct-access;
    file filename {
      checksum (md5 | sha-256 | sha1);
      optional;
      refresh;
      refresh-from url;
      source url;
    }
    refresh;
    refresh-from url;
    traceoptions {
      file {
        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
}
load-scripts-from-flash;
op {
  file filename {
    arguments name {
      description text;
    }
    checksum (md5 | sha-256 | sha1);
    command filename-alias;
    description cli-help-text;
    refresh;
    refresh-from url;
    source url;
  }
  no-allow-url;
  refresh;
  refresh-from url;
  traceoptions {
    file {
      filename;
      files number;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
  }
  flag flag;

```

```
        no-remote-trace;
    }
}
security-profile security-profile-name {
    address-book {
        maximum amount;
        reserved amount;
    }
    appfw-profile {
        maximum amount;
        reserved amount;
    }
    appfw-rule {
        maximum amount;
        reserved amount;
    }
    appfw-rule-set {
        maximum amount;
        reserved amount;
    }
    auth-entry {
        maximum amount;
        reserved amount;
    }
    cpu {
        reserved percent;
    }
    dslite-software-initiator {
        maximum amount;
        reserved amount;
    }
    flow-gate {
        maximum amount;
        reserved amount;
    }
    flow-session {
        maximum amount;
        reserved amount;
    }
    idp-policy idp-policy-name;
    logical-system logical-system-name;
    nat-cone-binding {
        maximum amount;
        reserved amount;
    }
    nat-destination-pool {
        maximum amount;
        reserved amount;
    }
    nat-destination-rule {
        maximum amount;
        reserved amount;
    }
    nat-interface-port-ol {
        maximum amount;
        reserved amount;
    }
}
```



```

    }
    nat-nopat-address {
        maximum amount;
        reserved amount;
    }
    nat-pat-address {
        maximum amount;
        reserved amount;
    }
    nat-pat-portnum {
        maximum amount
        reserved amount
    }
    nat-port-ol-ipnumber {
        maximum amount;
        reserved amount;
    }
    nat-rule-referenced-prefix {
        maximum amount;
        reserved amount;
    }
    nat-source-pool {
        maximum amount;
        reserved amount;
    }
    nat-source-rule {
        maximum amount;
        reserved amount;
    }
    nat-static-rule {
        maximum amount;
        reserved amount;
    }
    policy {
        maximum amount;
        reserved amount;
    }
    policy-with-count {
        maximum amount;
        reserved amount;
    }
    root-logical-system;
    scheduler {
        maximum amount;
        reserved amount;
    }
    zone {
        maximum amount;
        reserved amount;
    }
}
security-profile-resources {
    cpu-control;
    cpu-control-target percent;
}
services {

```

```

database-replication {
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}

dhcp {
  boot-file filename;
  boot-server (address | hostname);
  default-lease-time (infinite | seconds);
  domain-name domain-name;
  domain-search dns-search-suffix;
  maximum-lease-time (infinite | seconds);
  name-server ip-address;
  next-server ip-address;
  option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
    (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
    signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
    unsigned-short 16-bit-value);
  pool subnet-ip-address/mask {
    address-range {
      high address;
      low address;
    }
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (infinite | seconds);
    domain-name domain-name;
    domain-search dns-search-suffix;
    exclude-address ip-address;
    maximum-lease-time (infinite | seconds);
    name-server ip-address;
    next-server ip-address;
    option option-identifier-code array type-name [ type-values ] | byte 8-bit-value |
    flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
    short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
    unsigned-short 16-bit-value);
    propagate-ppp-settings interface-name;
    propagate-settings interface-name;
    router ip-address;
    server-identifier dhcp-server;
    sip-server {
      address ip-address;
      name sip-server-name;
    }
    wins-server ip-address;
  }
  propagate-ppp-settings interface-name;
  propagate-settings interface-name;
}

```

```

router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
static-binding mac-address;
traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
wins-server ip-address;
}
dhcp-local-server {
    dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
            }
        }
    }
}

```

```
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
    }
}
dynamic-profile {
    profile-name;
    aggregate-clients {
        merge;
        replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
}
interface interface-name {
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
        }
    }
}
```

```

        no-adaptation;
        session-mode (automatic | multihop | single-hop);
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;

```

```
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
group group-name {
    interface interface-name {
        exclude;
        upto upto-interface-name;
    }
}
}
dns {
    dns-proxy {
        cache hostname inet ip-address;
        default-domain domain-name {
            forwarders ip-address;
        }
        interface interface-name;
        propagate-setting (enable | disable);
        view view-name {
            domain domain-name {
                forward-only;
                forwarders ip-address;
            }
            match-clients subnet-address;
        }
    }
}
dnssec {
    disable;
    dlv {
        domain-name domain-name trusted-anchor trusted-anchor;
    }
    secure-domains domain-name;
    trusted-keys (key dns-key | load-key-file url);
    forwarders {
        ip-address;
    }
    max-cache-ttl seconds;
    max-ncache-ttl seconds;
    traceoptions {
        category {
            category-type;
        }
    }
}
```

```

    }
    debug-level level;
    file {
        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password server-password;
        server server-name;
        username user-name;
    }
}
finger {
    connection-limit number;
    rate-limit number;
}
ftp {
    connection-limit number;
    rate-limit number;
}
netconf {
    ssh {
        connection-limit number;
        port port-number;
        rate-limit number;
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
        on-demand;
    }
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout value;
        }
    }
}

```

```
device-id device-id;  
keep-alive {  
    retry number;  
    time-out value;  
}  
reconnect-strategy (in-order | sticky);  
secret secret;  
services {  
    netconf;  
}  
}  
tracoptions {  
    file {  
        filename;  
        files number;  
        match regular-expression;  
        size maximum-file-size;  
        (world-readable | no-world-readable);  
    }  
    flag flag;  
    no-remote-trace;  
}  
}  
service-deployment {  
    local-certificate certificate-name;  
    servers server-address {  
        port port-number;  
        security-options {  
            ssl3;  
            tls;  
        }  
        user user-name;  
    }  
    source-address source-address;  
    tracoptions {  
        file {  
            filename;  
            files number;  
            match regular-expression;  
            size maximum-file-size;  
            (world-readable | no-world-readable);  
        }  
        flag flag;  
        no-remote-trace;  
    }  
}  
}  
ssh {  
    ciphers [cipher];  
    client-alive-count-max number;  
    client-alive-interval seconds;  
    connection-limit number;  
    hostkey-algorithm {  
        (ssh-dss | no-ssh-dss);  
        (ssh-ecdsa | no-ssh-ecdsa);  
        (ssh-rsa | no-ssh-rsa);  
    }  
}
```



```

key-exchange [algorithm];
macs [algorithm];
max-sessions-per-connection number;
protocol-version {
    v1;
    v2;
}
rate-limit number;
root-login (allow | deny | deny-password);
(tcp-forwarding | no-tcp-forwarding);
}
subscriber-management {
    enforce-strict-scale-limit-license;
    gres-route-flush-delay;
    maintain-subscriber interface-delete;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
subscriber-management-helper {
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
telnet {
    connection-limit number;
    rate-limit number;
}
web-management {
    control {
        max-threads number;
    }
    http {
        interface [interface-name];
        port port-number;
    }
    https {
        interface [interface-name];
        local-certificate name;
        pki-local-certificate name;
    }
}

```

```
    port port-number;  
    system-generated-certificate;  
  }  
  management-url url;  
  session {  
    idle-timeout minutes;  
    session-limit number;  
  }  
  traceoptions {  
    file {  
      filename;  
      files number;  
      match regular-expression;  
      size maximum-file-size;  
      (world-readable | no-world-readable);  
    }  
    flag flag;  
    level (all | error | info | notice | verbose | warning);  
    no-remote-trace;  
  }  
}  
xnm-clear-text {  
  connection-limit number;  
  rate-limit number;  
}  
xnm-ssl {  
  connection-limit number;  
  local-certificate name;  
  rate-limit number;  
}  
}  
static-host-mapping hostname {  
  alias [host-name-alias];  
  inet [ip- address];  
  inet6 [ipv6- address];  
  sysid system-identifier;  
}  
syslog {  
  allow-duplicates;  
  archive {  
    binary-data;  
    files number;  
    size maximum-file-size;  
    (world-readable | no-world-readable);  
  }  
  console {  
    (any | facility) severity;  
  }  
  file filename {  
    allow-duplicates;  
    archive {  
      archive-sites url {  
        password password;  
      }  
      (binary-data | no-binary-data);  
      files number;  
    }  
  }  
}
```

```

        size maximum-file-size;
        start-time "YYYY-MM-DD.hh:mm";
        transfer-interval minutes;
        (world-readable | no-world-readable);
    }
    structure-data {
        brief;
    }
    (any | facility) severity;
}
host (hostname | other-routing-engine) {
    (any | facility) severity;
}
log-rotate-frequency minutes;
source-address source-address;
time-format {
    millisecond;
    year;
}
user (username | *) {
    (any | facility) severity;
}
}
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    service-name service-name;
}
tacplus-server server-address {
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
time-zone (GMThour-offset | time-zone);
tracing {
    destination-override {
        syslog {
            host address;
        }
    }
}
}
use-imported-time-zones;
}

```

address-assignment (Access)

```
Syntax address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-name;
    pool pool-name {
        family {
            inet {
                dhcp-attributes {
                    boot-file boot-file-name;
                    boot-server boot-server-name;
                    domain-name domain-name;
                    grace-period seconds;
                    maximum-lease-time (seconds | infinite);
                    name-server ipv4-address;
                    netbios-node-type (b-node | h-node | m-node | p-node);
                    next-server next-server-name;
                    option dhcp-option-identifier-code {
                        array {
                            byte [8-bit-value];
                            flag [ false | off | on | true ];
                            integer [32-bit-numeric-values];
                            ip-address [ip-address];
                            short [signed-16-bit-numeric-value];
                            string [character string value];
                            unsigned-integer [unsigned-32-bit-numeric-value];
                            unsigned-short [16-bit-numeric-value];
                        }
                        byte 8-bit-value;
                        flag (false | off | on | true);
                        integer 32-bit-numeric-values;
                        ip-address ip-address;
                        short signed-16-bit-numeric-value;
                        string character string value;
                        unsigned-integer unsigned-32-bit-numeric-value;
                        unsigned-short 16-bit-numeric-value;
                    }
                }
                byte 8-bit-value;
                flag (false | off | on | true);
                integer 32-bit-numeric-values;
                ip-address ip-address;
                short signed-16-bit-numeric-value;
                string character string value;
                unsigned-integer unsigned-32-bit-numeric-value;
                unsigned-short 16-bit-numeric-value;
            }
        }
        option-match {
            option-82 {
                circuit-id match-value {
                    range range-name;
                }
                remote-id match-value;
                range range-name;
            }
        }
    }
    propagate-ppp-settings [interface-name];
    propagate-settings interface-name;
    router ipv4-address;
    server-identifier ip-address;
}
```

```

sip-server {
    ip-address ipv4-address;
    name sip-server-name;
}
tftp-server server-name;
wins-server ipv4-address;
}
host hostname {
    hardware-address mac-address;
    ip-address reserved-address;
}
network network address;
range range-name {
    high upper-limit;
    low lower-limit;
}
excluded-range range-name
    high upper-limit;
    low lower-limit;
}
xauth-attributes {
    primary-dns ip-address;
    primary-wins ip-address;
    secondary-dns ip-address;
    secondary-wins ip-address;
}
}
inet6 {
    dhcp-attributes {
        dns-server ipv6-address;
        grace-period seconds;
        maximum-lease-time (seconds | infinite);
        option dhcp-option-identifier-code {
            array {
                byte [8-bit-value];
                flag [ false | off | on | true];
                integer [32-bit-numeric-values];
                ip-address [ip-address];
                short [signed-16-bit-numeric-value];
                string [character string value];
                unsigned-integer [unsigned-32-bit-numeric-value];
                unsigned-short [16-bit-numeric-value];
            }
            byte 8-bit-value;
            flag (false | off | on | true);
            integer 32-bit-numeric-values;
            ip-address ip-address;
            short signed-16-bit-numeric-value;
            string character string value;
            unsigned-integer unsigned-32-bit-numeric-value;
            unsigned-short 16-bit-numeric-value;
        }
        propagate-ppp-settings [interface-name];
        sip-server-address ipv6-address;
        sip-server-domain-name domain-name;
    }
}

```

```
    prefix ipv6-network-prefix;  
    range range-name {  
        high upper-limit;  
        low lower-limit;  
        prefix-length delegated-prefix-length;  
    }  
    excluded-range range-name  
        high upper-limit;  
        low lower-limit;  
    }  
    }  
    link pool-name;  
    }  
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Dynamic VPN Overview*

address-pool (Access)

Syntax	<pre> address-pool <i>pool-name</i> { address <i>address or address prefix</i>; address-range { high <i>upper-limit</i>; low <i>lower-limit</i>; mask <i>network-mask</i>; } primary-dns <i>IP address</i>; primary-wins <i>IP address</i>; secondary-dns <i>IP address</i>; secondary-wins <i>IP address</i>; } </pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Create an address-pool for L2TP clients.
Options	<ul style="list-style-type: none"> • pool-name—Name assigned to the address-pool. • address—Configure subnet information for the address-pool. • address-range—Defines the address range available for clients. • primary-dns—Specify the primary-dns IP address. • secondary-dns—Specify the secondary-dns IP address. • primary-wins—Specify the primary-wins IP address. • secondary-wins—Specify the secondary-wins IP address.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • access-control on page 842

allow-configuration

Syntax	<code>allow-configuration "regular-expression";</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.2 for SRX Series devices.
Description	Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement do not grant such access by default.
Default	If you omit this statement and the deny-configuration statement, users can edit only those commands for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

allow-configuration-regexps

Syntax	<code>allow-configuration-regexps "regular expression 1" "regular expression 2";</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access. The statement deny-configuration-regexps takes precedence if it is used in the same login class definition.
Default	If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement.
Options	<i>regular expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

authentication-key

Syntax	<code>authentication-key <i>key-number</i> type <i>md5</i> value <<i>password</i>>;</code>
Hierarchy Level	[edit system <i>ntp</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure Network Time Protocol (NTP) authentication keys so that the SRX Series device can send authenticated packets. If you configure the SRX Series device to operate in authenticated mode, you must configure a key.</p> <p>Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.</p>
Options	<p><i>key-number</i>—Positive integer that identifies the key.</p> <p><i>type md5</i>—Authentication type. It can only be <i>md5</i>.</p> <p><i>value password</i>—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • ntp on page 1248

authentication-order

Syntax	<code>authentication-order [<i>authentication-methods</i>];</code>
Hierarchy Level	<code>[edit system]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
Default	If you do not include the authentication-order statement, users are verified based on their configured passwords.
Options	<i>authentication-methods</i> —One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following: <ul style="list-style-type: none">• password—Use the password configured for the user with the authentication statement at the <code>[edit system login user]</code> hierarchy level.• radius—Use RADIUS authentication services.• tacplus—Use TACACS+ authentication services.
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding User Authentication Methods on page 804

boot-server (NTP)

Syntax	<code>boot-server (address hostname);</code>
Hierarchy Level	[edit system <i>ntp</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the server that NTP queries when the SRX Series device boots to determine the local date and time.</p> <p>When you boot the SRX Series device, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the SRX Series device uses to determine the time when the SRX Series device boots. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the ntpdate request resolves the hostname to an IP address when the SRX Series device boots up.</p> <p>If you configure an NTP boot server, then when the SRX Series device boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.</p>
Options	<ul style="list-style-type: none">• address—The IP address of an NTP boot server.• hostname—The hostname of an NTP boot server.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248


broadcast

Syntax	<code>broadcast address <key key-number> <routing-instance-name routing-instance-name> <ttl value> <version value>;</code>
Hierarchy Level	[edit system <i>ntp</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the SRX Series device to operate in broadcast mode with the remote system at the specified address. In this mode, the SRX Series device sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Normally, you include this statement only when the SRX Series device is operating as a transmitter.
Options	<p>address—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be 224.0.1.1.</p> <p>key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p>Range: Any unsigned 32-bit integer</p> <p>routing-instance-name routing-instance-name—(Optional) The routing instance name in which the interface has an address in the broadcast subnet.</p> <p>Default: The default routing instance is used to broadcast packets.</p> <p>ttl value—(Optional) Time-to-live (TTL) value to use.</p> <p>Range: 1 through 255</p> <p>Default: 1</p> <p>version value—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248


broadcast-client

Syntax	<code>broadcast-client;</code>
Hierarchy Level	<code>[edit system <i>ntp</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the SRX Series device to listen for broadcast messages on the local network to discover other servers on the same subnet.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248

ciphers

Syntax	<code>ciphers [cipher-1 cipher-2 cipher-3 ...]</code>
Hierarchy Level	<code>[edit system services ssh]</code>
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.
Options	<ul style="list-style-type: none"> • 3des-cbc—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode. • aes128-cbc—128-bit Advanced Encryption Standard (AES) in CBC mode. • aes256-cbc—256-bit AES in CBC mode. • aes128-ctr—128-bit AES in CBC mode. • aes192-ctr—192-bit AES in counter mode. • aes256-ctr—256-bit AES in counter mode. • aes128-gcm@openssh.com—128-bit AES in Galois/Counter Mode. • aes256-gcm@openssh.com—256-bit AES in Galois/Counter Mode. • arcfour128—128-bit RC4-stream cipher in CBC mode. • arcfour256—256-bit RC4-stream cipher in CBC mode. • blowfish128-cbc—128-bit blowfish-symmetric block cipher in CBC mode. • cast128-cbc—128-bit cast in CBC mode.
<div>  <p>NOTE: Ciphers represent a set. To configure SSH ciphers:</p> <pre>user@host#set system services ssh ciphers [aes256-cbc aes192-cbc]</pre> </div>	
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring SSH Service for Remote Access to the Router or Switch</i>

connection-limit

Syntax	connection-limit <i>limit</i> ;
Hierarchy Level	[edit system services finger] [edit system services ftp] [edit system services netconf ssh] [edit system services ssh] [edit system services telnet] [edit system services xnm-clear-text] [edit system services xnm-ssl]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure the maximum number of connection sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).
Options	<p>limit—Maximum number of established connections per protocol (either IPv6 or IPv4).</p> <p>On all high-end SRX Series devices, the range and default value are as follows: Range: 1 through 250 Default: 75</p> <p>On all branch SRX Series devices, the range is as follows: Range: 1 through 5</p>
<div>  <p>NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.</p> </div>	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

client-ia-type

Syntax	client-ia-type (ia-na ia-pd);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Configure the DHCPv6 client identity association type.
Options	ia-na — Identity association for nontemporary address ia-pd —Identity association for prefix delegation
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCPv6 Client Overview on page 1120

client-identifier (dhcp-client)

Syntax	client-identifier { user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i> ; use-interface-description {logical device}; prefix [host-name routing-instance-name]; }
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	The DHCP server identifies a client by a client-identifier value.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCPv6 Client Overview on page 1120

client-identifier (dhcpv6-client)

Syntax	client-identifier duid-type (duid-ll duid-llt vendor);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	The DHCPv6 server identifies a client by a client-identifier value.
Options	<p>duid-type—The DHCPv6 client is identified by a DHCP unique identifier (DUID).</p> <p>duid-ll—Link Layer address.</p> <p>duid-llt—Link Layer address plus time.</p> <p>vendor—Vendor-assigned unique ID based on the enterprise number.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCPv6 Client Overview on page 1120

client-list-name (SNMP)

Syntax	client-list-name <i>client-list-name</i> ;
Hierarchy Level	[edit snmp community <i>community-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration.
Options	client-list-name — Name of the client list. Client list is the list of IP address prefixes defined with the prefix-list statement in the policy-options hierarchy.
Required Privilege Level	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding the SNMP Implementation in Junos OS • Standard SNMP MIBs Supported by Junos OS on page 1409

client-type

Syntax	client-type (autoconfig statefull);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	The type of DHCPv6 client.
Options	<ul style="list-style-type: none">• autoconfig—Autoconfig client type for router advertisement• statefull—Stateful client type for address assignment
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCPv6 Client Overview on page 1120

deny-configuration

Syntax	deny-configuration " <i>regular-expression</i> ";
Hierarchy Level	[edit system login class]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.2 for SRX Series devices.
Description	Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement grant such access by default.
Default	If you omit this statement and the allow-configuration statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the permissions statement.
Options	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

deny-configuration-regexps

Syntax	<code>deny-configuration-regexps "regular expression 1" "regular expression 2";</code>
Hierarchy Level	[edit system login class <i>class-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.2 for SRX Series devices.
Description	<p>Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access.</p> <p>Expressions configured with this statement take precedence over allow-configuration-regexps if the two statements are used in the same login class definition.</p>
Default	If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement.
Options	<p><i>regular expression</i>—Extended (modern) regular expression as defined in POSIX 1003.2.</p> <p>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

destination (Accounting)

```
Syntax  destination {  
        radius {  
            server {  
                server-address {  
                    accounting-port port-number;  
                    max-outstanding-requests value;  
                    port port-number;  
                    retry value;  
                    secret password;  
                    source-address source-address;  
                    timeout seconds;  
                }  
            }  
        }  
        tacplus {  
            server {  
                server-address {  
                    port port-number;  
                    secret password;  
                    single-connection;  
                    timeout seconds;  
                }  
            }  
        }  
    }
```

Hierarchy Level [edit system accounting]

Release Information Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4. Support for IPv6 source address added in Junos OS Release 12.1X47-D15.

Description Configure the authentication server.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

dhcp-attributes (Access IPv4 Address Pools)

```
Syntax  dhcp-attributes {
    boot-file boot-file-name;
    boot-server boot-server-name;
    domain-name domain-name;
    grace-period seconds;
    maximum-lease-time (seconds | infinite);
    name-server ipv4-address;
    netbios-node-type (b-node | h-node | m-node | p-node);
    next-server next-server-name;
    option dhcp-option-identifier-code {
        array {
            byte [8-bit-value];
            flag [ false | off | on | true];
            integer [32-bit-numeric-values];
            ip-address [ip-address];
            short [signed-16-bit-numeric-value];
            string [character string value];
            unsigned-integer [unsigned-32-bit-numeric-value];
            unsigned-short [16-bit-numeric-value];
        }
        byte 8-bit-value;
        flag ( false | off | on | true);
        integer 32-bit-numeric-values;
        ip-address ip-address;
        short signed-16-bit-numeric-value;
        string character string value;
        unsigned-integer unsigned-32-bit-numeric-value;
        unsigned-short 16-bit-numeric-value;
    }
    option-match {
        option-82 {
            circuit-id match-value {
                range range-name;
            }
            remote-id match-value;
            range range-name;
        }
    }
    propagate-ppp-settings [interface-name];
    propagate-settings interface-name;
    router ipv4-address;
    server-identifier ip-address;
    sip-server {
        ip-address ipv4-address;
        name sip-server-name;
    }
    tftp-server server-name;
    wins-server ipv4-address;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet]

Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Server, Client, and Relay Agent Overview on page 1088

dhcp-attributes (Access IPv6 Address Pools)

Syntax

```
dhcp-attributes {
  dns-server ipv6-address;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [ false | off | on | true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag ( false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  propagate-ppp-settings [interface-name];
  sip-server-address ipv6-address;
  sip-server-domain-name domain-name;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet6]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure attributes for address pools that can be used by different clients.

- Options**
- **dns-server *IPv6-address***—Specify a DNS server to which clients can send DNS queries.
 - **grace-period *seconds***—Specify the grace period offered with the lease.

Range: 0 through 4,294,967,295 seconds

Default: 0 (no grace period)

- **maximum-lease-time *seconds***—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

Range: 30 through 4,294,967,295 seconds

Default: 86,400 seconds (24 hours)

- **option *dhcp-option-identifier-code***—Specify the DHCP option identifier code.
- **propagate-ppp-settings [*interface-name*]**—Specify PPP interface name for propagating DNS or WINS settings.

- **sip-server-address** *IPv6-address*—Specify the IPv6 address of the SIP outbound proxy server.
- **sip-server-domain-name** *domain-name*—Specify the domain name of the SIP outbound proxy server.

Required Privilege Level access—To view this statement in the configuration.
 access-control—To add this statement to the configuration.

Related Documentation • [DHCP Server, Client, and Relay Agent Overview on page 1088](#)

dhcp-client

Syntax dhcp-client {
 client-identifier {
 prefix {
 host-name;
 logical-system-name;
 routing-instance-name;
 }
 use-interface-description (device | logical);
 user-id (ascii *string* | hexadecimal *string*);
 }
 lease-time (*length* | infinite);
 retransmission-attempt *value*;
 retransmission-interval *seconds*;
 server-address *server-address*;
 update-server;
 vendor-id *vendor-id* ;
 }

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation • [DHCP Server, Client, and Relay Agent Overview on page 1088](#)

dhcp-local-server (System Services)

```

Syntax  dhcp-local-server {
        dhcpv6 {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        group group-name {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile;
        }
    }

```

```
}
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
```

```

reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}

```

```
group group-name {  
  interface interface-name {  
    exclude;  
    upto upto-interface-name;  
  }  
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.



NOTE: SRX Series devices do not support client authentication.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)

dhcpv6 (System Services)

```
Syntax  dhcpv6 {
    authentication {
        password password;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name;
            interface-name;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile;
        }
    }
}
```

```
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
reconfigure {
```

```

        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}

```

Hierarchy Level	[edit system services]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure DHCPv6 server to provide IPv6 addresses to clients.



NOTE: SRX Series devices do not support client authentication.

Options	<ul style="list-style-type: none"> duplicate-clients-on-interface—Allow duplicate clients on different interfaces in a subnet. <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> DHCP Server, Client, and Relay Agent Overview on page 1088

dhcpv6-client

Syntax	<pre>dhcpv6-client { client-ia-type (ia-na ia-pd); client-identifier duid-type (duid-ll duid-llt vendor); client-type (autoconfig statefull); rapid-commit; req-option (dns-server domain fqdn nis-domain nis-server ntp-server sip-domain sip-server time-zone vendor-spec); retransmission-attempt <i>number</i>; update-router-advertisement { interface <i>interface-name</i>; } update-server; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Configure the Dynamic Host Configuration Protocol version 6 (DHCPv6) client.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> DHCP Server, Client, and Relay Agent Overview on page 1088

disable (System Services)

Syntax	disable;
Hierarchy Level	[edit system services dns dnssec]
Release Information	Statement introduced in Junos OS Release 10.2 .
Description	Disables DNSSEC in the DNS server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Server, Client, and Relay Agent Overview on page 1088

dlv

Syntax	<pre>dlv { domain-name <i>domain-name</i> trusted-anchor <i>trusted-anchor</i>; }</pre>
Hierarchy Level	[edit system services dns dnssec]
Release Information	Statement introduced in Junos OS Release 10.2 .
Description	Configure DNSSEC Lookaside Validation (DLV).
Options	<ul style="list-style-type: none"> • domain-name <i>domain-name</i>—Specify the secure domain server name. • trusted-anchor <i>trusted-anchor</i>—Specify the trusted DLV anchor.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Server, Client, and Relay Agent Overview on page 1088

family (Security Forwarding Options)

Syntax

```
family {  
  inet6 {  
    mode (drop | flow-based | packet-based);  
  }  
  iso {  
    mode packet-based;  
  }  
  mpls {  
    mode packet-based;  
  }  
}
```

Hierarchy Level [edit security forwarding-options]

Release Information Statement introduced in Junos OS Release 8.5 .

Description Determine the protocol family to be used for packet forwarding.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

security	—To view this statement in the configuration.
security-control	—To add this statement to the configuration.

Related Documentation

- *MPLS Overview*

file (System Logging)

Syntax file *filename* {
 allow-duplicates;
 any (alert | any | critical | emergency | error | info | none | notice | warning);
 archive {
 archive-sites {
 url *password*;
 }
 (binary-data | no-binary-data);
 files *number*;
 size *size*;
 start-time *start-time*;
 transfer-interval *transfer-interval*;
 (world-readable | no-world-readable);
 }
 authorization (alert | any | critical | emergency | error | info | none | notice | warning);
 change-log (alert | any | critical | emergency | error | info | none | notice | warning);
 conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
 daemon (alert | any | critical | emergency | error | info | none | notice | warning);
 dfc (alert | any | critical | emergency | error | info | none | notice | warning);
 explicit-priority;
 external (alert | any | critical | emergency | error | info | none | notice | warning);
 firewall (alert | any | critical | emergency | error | info | none | notice | warning);
 ftp (alert | any | critical | emergency | error | info | none | notice | warning);
 interactive-commands (alert | any | critical | emergency | error | info | none | notice | warning);
 kernel (alert | any | critical | emergency | error | info | none | notice | warning);
 match "*regular-expression*";
 ntp (alert | any | critical | emergency | error | info | none | notice | warning);
 pfe (alert | any | critical | emergency | error | info | none | notice | warning);
 security (alert | any | critical | emergency | error | info | none | notice | warning);
 structured-data {
 brief;
 }
 user (alert | any | critical | emergency | error | info | none | notice | warning);
 }

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

- Options**
- *filename*—Specify the name of the file in which to log data.
 - *allow-duplicates*—Do not suppress the repeated messages.
 - *any*—Specify all facilities information.
 - *alert*—Specify the conditions that should be corrected immediately.
 - *critical*—Specify the critical conditions.
 - *emergency*—Specify the conditions that cause security functions to stop.
 - *error*—Specify the general error conditions.

- *info*—Specify the information about normal security operations.
- *none*—Do not specify any messages.
- *notice*—Specify the conditions that should be handled specifically.
- *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
 - *archive-sites*—Specify a list of destination URLs for the archived log files.
 - *url*—Specify the primary and failover URLs to receive archive files.
 - *binary-data*—Mark file such that it contains binary data.
 - *no-binary-data*—Do not mark the file such that it contains binary data.
 - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
 - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
 - *world-readable*—Allow any user to read the log file.
 - *no-world-readable*—Do not allow any user to read the log file.
 - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
 - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.
- *pfe*—Specify the Packet Forwarding Engine.
- *security*—Specify the security-related information.

- *structured-data*—Log the messages in structured log format.
 - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
 - *info*—Specify the informational messages.

Required Privilege	system—To view this statement in the configuration.
Level	system-control—To add this statement to the configuration.

forwarding-options (Security)

Syntax

```
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.

Description Determine how the **inet6**, **iso**, and **mpls** protocol families manage security forwarding options.



NOTE:

- Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.
- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the `set security forwarding-options family mpls mode packet-based` statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *MPLS Overview*
- *Understanding Packet-Based Processing*
- *Juniper Networks Devices Processing Overview*

group (System Services DHCP)

```

Syntax  group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile;
        }
        interface interface-name {
            dynamic-profile {
                profile-name;
                aggregate-clients {
                    merge;
                    replace;
                }
                junos-default-profile;
                use-primary dynamic-profile-name;
            }
            exclude;
            overrides {
                delegated-pool pool-name;
                interface-client-limit number;
                process-inform {
                    pool pool-name;
                }
                rapid-commit ;
            }
            service-profile service-profile-name
            trace ;
            upto interface-name;
        }
        liveness-detection {
            failure-action {
                clear-binding;
            }
        }
    }

```

```

        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
}
service-profile service-profile-name;
}

```

Hierarchy Level [edit system services dhcp-local-server dhcpv6]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a group of interfaces that have a common configuration.

The remaining statements are explained separately. See [CLI Explorer](#).

- Options**
- *group-name*—Name of the group.



NOTE: SRX Series devices do not support DHCP client authentication.

The remaining statements are explained separately. See [CLI Explorer](#).


Required Privilege	access—To view this statement in the configuration.
Level	access-control—To add this statement to the configuration.

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• DHCP Server, Client, and Relay Agent Overview on page 1088• DHCP Server Configuration Overview on page 1092 |
|------------------------------|--|

host (SSH Known Hosts)

Syntax	<pre>host <i>hostname</i> { dsa-key <i>dsa-key</i>; ecdsa-sha2-nistp256-key <i>ecdsa-sha2-nistp256-key</i>; ecdsa-sha2-nistp384-key <i>ecdsa-sha2-nistp384-key</i>; ecdsa-sha2-nistp521-key <i>ecdsa-sha2-nistp521-key</i>; rsa-key <i>rsa-key</i>; rsa1-key <i>rsa1-key</i>; }</pre>
Hierarchy Level	[edit security ssh-known-hosts]
Release Information	Statement modified in Junos OS Release 8.5.
Description	Configure the type of base-64 encoded host key.
Options	<ul style="list-style-type: none">• <i>hostname</i>—Name of the SSH known host.• <i>dsa-key dsa-key</i>—Digital Signature Algorithm (DSA) for SSH version 2• <i>ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key</i>—Elliptic Curve Digital Signature Algorithm (ECDSA)• <i>ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key</i>—Elliptic Curve Digital Signature Algorithm (ECDSA)• <i>ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key</i>—Elliptic Curve Digital Signature Algorithm (ECDSA)• <i>rsa-key rsa-key</i>—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2• <i>rsa1-key rsa1-key</i>—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Generating an SSL Certificate Using the openssl Command on page 1028• Generating a Self-Signed SSL Certificate on page 1028

hostkey-algorithm

Syntax	hostkey-algorithm <i><algorithm no-algorithm></i>
Hierarchy Level	[edit system services ssh]
Release Information	Statement introduced in Junos OS Release 11.2. <i><algorithm no algorithm></i> statements introduced in Junos OS Release 12.2.
Description	Allow or disallow a host-key signature algorithm for the SSH host to use to authenticate another host.
Options	<ul style="list-style-type: none"> • no-ssh-dss—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key. • no-ssh-ecdsa—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key. • no-ssh-rsa—Do not allow generation of an RSA host-key. • ssh-ecdsa—Allow generation of an ECDSA host-key. • ssh-dss—Allow generation of a 1024-bit DSA host-key.
	<div>  <p>NOTE: DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode.</p> </div>
	<ul style="list-style-type: none"> • ssh-rsa—Allow generation of an RSA host-key.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Generating an SSL Certificate Using the openssl Command on page 1028 • Generating a Self-Signed SSL Certificate on page 1028

interface (System Services DHCP)

Syntax	<pre>interface <i>interface-name</i> { exclude; overrides { interface-client-limit <i>number</i>; } trace; upto <i>upto-interface-name</i>; }</pre>
Hierarchy Level	[edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.
Options	<ul style="list-style-type: none">• <i>interface-name</i>—Name of the interface.• trace—Enable tracing of the interface specified by the <i>interface-name</i> argument.• upto <i>upto-interface-name</i>—The upper end of the range of interfaces; the lower end of the range is the <i>interface-name</i> entry. The interface device name of the <i>upto-interface-name</i> must be the same as the device name of the <i>interface-name</i>.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Server, Client, and Relay Agent Overview on page 1088• DHCP Server Configuration Overview on page 1092

interfaces (ARP)

Syntax	<pre>interfaces { <i>interface-name</i> { aging-timer <i>minutes</i>; } }</pre>
Hierarchy Level	[edit system arp]
Release Information	Statement introduced before Junos OS Release 9.4.
Description	Specify the Address Resolution Protocol (ARP) aging timer in minutes for a logical interface.
Options	<p>aging-timer <i>minutes</i>—Time between ARP updates, in minutes.</p> <p>Range: 1 through 240</p> <p>Default: 20</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• DHCP Server, Client, and Relay Agent Overview on page 1088• DHCP Server Configuration Overview on page 1092

interfaces (Security Zones)

Syntax	<pre>interfaces <i>interface-name</i> { host-inbound-traffic { protocols <i>protocol-name</i> { except; } } system-services <i>service-name</i> { except; } }</pre>
Hierarchy Level	[edit security zones functional-zone management], [edit security zones security-zone <i>zone-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the set of interfaces that are part of the zone.
Options	<i>interface-name</i> —Name of the interface. The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Understanding Security Zones</i>

interface-traceoptions (System Services DHCP)

Syntax	<pre> interface-traceoptions { file { filename ; files number; match regular-expression; size maximum-file-size; (world-readable no-world-readable); } flag flag; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the interface <i>interface-name</i> trace statement at the [edit system services group <i>group-name</i>] hierarchy level to enable the tracing operation on the specific interfaces.
Options	<p>file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named jdhcpd in the directory /var/log. If you include the file statement, you must specify a filename.</p> <p>files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all events • dhcpv6-packet—Trace DHCPv6 packet decoding operations. • dhcpv6-packet-option—Trace DHCPv6 option decoding operations. • dhcpv6-state—Trace changes in state for DHCPv6 operations. • packet—Trace packet decoding operations • packet-option—Trace DHCP option decoding operations • state—Trace changes in state

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	• DHCP Server, Client, and Relay Agent Overview on page 1088
	• DHCP Server Configuration Overview on page 1092

internet-options

Syntax

```
internet-options {
    icmpv4-rate-limit {
        bucket size seconds;
        packet-rate packet-rate;
    }
    icmpv6-rate-limit {
        bucket size seconds;
        packet-rate packet-rate;
    }
    ipv6-duplicate-addr-detection-transmits number;
    no-path-mtu-discovery;
    no-source-quench;
    no-tcp-reset;
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    path-mtu-discovery;
    source-port {
        upper-limit range;
    }
    source-quench;
    tcp-drop-synfin-set;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure tunable options for Internet operations.

- Options**
- **icmpv4-rate-limit**—Configure rate-limiting parameters for Internet Control Message Protocol version 4 (ICMPv4) messages.
 - **bucket-size *seconds***—Set ICMP rate-limiting maximum bucket size in seconds.
 - **packet-rate *packet-rate***— Set ICMP rate-limiting packets earned per second.
 - **icmpv6-rate-limit**—Configure rate-limiting parameters for Internet Control Message Protocol version 6 (ICMPv6) messages.
 - **bucket-size *seconds***—Set ICMP rate-limiting maximum bucket size in seconds.
 - **packet-rate *packet-rate***— Set ICMP rate-limiting packets earned per second.
 - **ipv6-duplicate-addr-detection-transmits *number***—Control the number of attempts for IPv6 duplicate address detection.
 - **no-path-mtu-discovery**—Do not enable path maximum transmission unit (MTU) discovery on TCP connections.
 - **no-source-quench**—Do not react to incoming ICMP source quench messages.
 - **no-tcp-reset**—Do not send RST TCP packets for packets sent to non-listening ports.
 - **no-tcp-rfc1323**—Disable RFC 1323 TCP extensions.

- **no-tcp-rfc1323-paws**—Disable RFC 1323 Protection Against Wrapped Sequence Number extension.
- **path-mtu-discovery**—Enable path MTU discovery on TCP connections.
- **source-port**—Configure source port selection parameters.
 - **upper-limit *range***—Specify upper limit of source port selection range.
- **source-quench**—React to incoming ICMP source quench messages.
- **tcp-drop-synfin-set**—Drop TCP packets that have both SYN and FIN flags.

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

kernel-replication (System)

Syntax kernel-replication;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure kernel replication.

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

lease-time (dhcp-client)

Syntax lease-time *seconds*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options **seconds**— Request time to negotiate and exchange information.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)


location

Syntax	<pre>location { altitude <i>feet</i>; building <i>name</i>; country -code <i>code</i>; floor <i>number</i>; hcoord <i>horizontal-coordinate</i>; lata <i>service-area</i>; latitude <i>degrees</i>; longitude <i>degrees</i>; npa-nxx <i>number</i>; postal-code <i>postal-code</i>; rack <i>number</i>; vcoord <i>vertical-coordinate</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Configure the physical location of the device.
Options	<ul style="list-style-type: none"> • altitude <i>feet</i>—Number of feet above sea level. • building <i>name</i>—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" "). • country-code <i>code</i>—Two-letter country code. • floor <i>number</i>—Floor number in the building. • hcoord <i>horizontal-coordinate</i>—Bellcore Horizontal Coordinate. • lata <i>service-area</i>—Long-distance service area. • latitude <i>degrees</i>—Latitude in degree format. • longitude <i>degrees</i>—Longitude in degree format. • npa-nxx <i>number</i>—First six digits of the phone number (area code and exchange). • postal-code <i>postal-code</i>—Zip code or Postal code. • rack <i>number</i>—Rack number. • vcoord <i>vertical-coordinate</i>—Bellcore Vertical Coordinate.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

lockout-period

Syntax	lockout-period <i>minutes</i> ;
Hierarchy Level	[edit system login retry-options]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Configure the amount of time before the user can attempt to log in to the router after being locked out due to the number of failed login attempts specified in the tries-before-disconnect statement.
Options	<i>minutes</i> —Amount of time before the user can attempt to log in after being locked out. Default: Off Range: 1 through 43200
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Limiting the Number of User Login Attempts for SSH and Telnet Sessions</i>• Handling Authorization Failure on page 822• Example: Configuring System Retry Options on page 823• <i>retry-options</i>• clear system login lockout on page 291• show system login lockout on page 409

macs

Syntax	<code>macs [algorithm]</code>
Hierarchy Level	<code>[edit system services ssh]</code>
Release Information	Statement introduced in Junos OS Release 11.2. SHA-2 options introduced in Junos OS Release 12.1.
Description	Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.
Options	<ul style="list-style-type: none"> • <code>hmac-md5</code>—Hash-based MAC using Message-Digest 5 (MD5). • <code>hmac-md5-96</code>—96-bits of Hash-based MAC using MD5. • <code>hmac-ripemd160</code>—Hash-based MAC using RIPEMD. • <code>hmac-sha1</code>—Hash-based MAC using Secure Hash Algorithm (SHA-1). • <code>hmac-sha1-96</code>—96-bits of Hash-based MAC using SHA-1. • <code>hmac-sha2-256</code>—256-bits of Hash-based MAC using SHA-2. • <code>hmac-sha2-256-96</code>—first 96-bits of hmac-sha2-256. • <code>hmac-sha2-512</code>—96-bits of Hash-based MAC using SHA-1. • <code>umac-64</code>—Message Authentication Code using Universal Hashing.
<div>  <p>NOTE: The <i>macs</i> configuration statement represents a set. Therefore, it should be configured as in the following.</p> <pre>user@host#set system services ssh macs [hmac-md5 hmac-sha1]</pre> </div>	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 1165

max-pre-authentication-packets

Syntax	<code>max-pre-authentication-packets <i>value</i>;</code>
Hierarchy Level	[edit system services ssh]
Release Information	Statement introduced in Junos OS Release 12.3X48-D10.
Description	Define the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication.
Options	<i>value</i> —Maximum number of pre-authentication SSH packets that the server will accept. Range: 20 through 2147483647. Default: 128
Required Privilege Level	admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• The ssh Command on page 1063

multicast-client

Syntax	<code>multicast-client <<i>address</i>>;</code>
Hierarchy Level	[edit system ntp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For NTP, configure the SRX Series device to listen for multicast messages on the local network to discover other servers on the same subnet.
Options	<i>address</i> —(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups. Default: 224.0.1.1.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248

name-server (Access)

Syntax	<code>name-server address</code>
Hierarchy Level	[edit access address-assignment pool <name> family (inet inet6) xauth-attributes]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the DNS server IP address for an address-assignment pool.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • address-assignment (Access) on page 1196 • <i>Access Configuration Statement Hierarchy</i>

neighbor-discovery-router-advertisement (Access)

Syntax	<code>neighbor-discovery-router-advertisement <i>ndra-pool-name</i>;</code>
Hierarchy Level	[edit access address-assignment]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure the name of the address-assignment pool used to assign the router advertisement prefix.
Options	<i>ndra-pool-name</i> —Name of the address assignment pool.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Access Configuration Statement Hierarchy</i>

ntp

Syntax ntp {
 authentication-key *key-number* type *md5* value *<password>*;
 boot-server *<address>*;
 broadcast *<address>* *<key key-number>* *<routing-instance routing-instance-name>* *<version value>* *<ttl value>*;
 broadcast-client;
 multicast-client *<address>*;
 peer *address* *<key key-number>* *<version value>* *<prefer>*;
 server *address* *<key key-number>* *<version value>* *<prefer>*;
 source-address *source-address* *<routing-instance routing-instance-name>*;
 trusted-key [*key-numbers*];
 }

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Network Time Protocol (NTP) on the SRX Series device.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

outbound-ssh

Syntax

```

outbound-ssh {
  client client-id {
    address address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}

```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.4.
Support for IPv6 address added in Junos OS Release 12.1X47-D15.

Description Initiate outbound SSH connections.

Options **client *client-id***—Defines a device-initiated connection. This value serves to uniquely identify the outbound-ssh configuration stanza. Each outbound-ssh stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the client-id any meaningful unique value.

address *address*—Specifies the IPv4 or IPv6 address or hostname of the client.

port *port-number*—Specifies the port at which a server listens for outbound SSH connection requests.

retry *number*—Specifies the maximum number of connection attempts a device can make to the specified IP address. The default is three attempts.

timeout *seconds*—Specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

device *device-id*—Identifies the device to the management client. Each time the device establishes an outbound SSH connection, it first sends an initiation sequence (device-id) to the management client.

keep-alive—Enables the device to send SSH protocol keepalive messages to the client application. The **timeout** statement specifies how long the device waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds. The **retry** statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the device disconnects from the application, ending the outbound SSH connection. The default is three retries.

reconnect-strategy (in-order|sticky)—Specifies how the device reconnects to the server after a connection is dropped.

in-order—Configures the device to reconnect to the first configured server. If this server is unavailable, the device tries to connect to the next configured server. This process repeats until a connection is completed.

sticky—Configures the device to reconnect to the server from which it disconnected.

secret password—Sends the device's public SSH host key when the device connects to the client.

services netconf—Configures the application to accept NETCONF as an available service.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• traceoptions (Outbound SSH) on page 1274• Configuring Outbound SSH Service on page 1064
------------------------------	--

overrides (System Services DHCP)

Syntax	<pre>overrides { interface-client-limit <i>number</i>; }</pre>
Hierarchy Level	<pre>[edit system services dhcp-local-server dhcpv6] [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>] [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>]</pre>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	<p>Override the default configuration settings for the extended DHCP local server. Specifying the overrides statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.</p> <ul style="list-style-type: none"> To override global DHCP local server configuration options, include the overrides statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level. To override configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>] hierarchy level. To override configuration options for a specific interface within a named group of interfaces, include the statements at the [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>] hierarchy level. Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.
Options	<p>interface-client-limit <i>number</i>—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.</p> <p>Range: 1 through 500,000</p> <p>Default: No limit</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> DHCP Server, Client, and Relay Agent Overview on page 1088

peer (NTP)

Syntax	<code>peer address <key key-number> <version value> <prefer>;</code>
Hierarchy Level	[edit system ntp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For NTP, configure the SRX Series device to operate in symmetric active mode with the remote system at the specified address. In this mode, the SRX Series device and the remote system can synchronize with each other. This configuration is useful in a network in which either the SRX Series device or the remote system might be a better source of time.
Options	<p>address—Address of the remote system. You must specify an address, not a hostname.</p> <p>key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p>Range: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version value—(Optional) Specify the NTP version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248

prefix

Syntax	<pre>prefix { host-name; logical-system-name; routing-instance-name; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify a prefix as a client identifier.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

profiller

Syntax	<pre>profiller { command <i>binary-file-path</i>; disable; failover (alternate-media other-routing-engine); }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the profiler process.
Options	<ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to binary for process. • disable—Disable the profiler process. • failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot. <ul style="list-style-type: none"> • alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly. • other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

proxy

Syntax	<pre>proxy { password <i>password</i>; port <i>port-number</i>; server <i>url</i>; username <i>user-name</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the proxy information for the router.
Options	<ul style="list-style-type: none">• password <i>password</i>—Password configured in the proxy server.• port <i>port number</i>—Proxy server port number. Range: 0 through 65,535• server <i>url</i>—URL or IP address of the proxy server host.• username <i>username</i>—Username configured in the proxy server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

radius-options

Syntax	<pre>radius-options { attributes { nas-ip-address <i>nas-ip-address</i>; } password-protocol mschap-v2; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5. Support for network access server (NAS) IPv6 address added in Junos OS Release 12.1X47-D15.
Description	Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.
Options	<ul style="list-style-type: none"> • attributes—Configure RADIUS attributes. <ul style="list-style-type: none"> • nas-ip-address <i>nas-ip-address</i>—Valid IPv4 or IPv6 address of the NAS requesting user authentication. • password-protocol mschap-v2—Protocol MS-CHAPv2, used for password authentication and password changing.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • radius-server on page 1256

radius-server

Syntax	<pre>radius-server server-address { accounting-port <i>port-number</i>; max-outstanding-requests <i>value</i>; port <i>port-number</i>; retry <i>value</i>; secret <i>password</i>; source-address <i>source-address</i>; timeout <i>seconds</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5. Support for IPv6 source address added in Junos OS Release 12.1X47-D15.
Description	<p>Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
Options	<ul style="list-style-type: none">• server-address—Address of the RADIUS server.• accounting-port <i>port-number</i>—RADIUS server accounting port number. Range: 1 through 65,335 files Default: 1813• port <i>port-number</i>—RADIUS server authentication port number. Range: 1 through 65,335 files Default: 1812• retry <i>value</i>—Number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 10 Default: 3• secret <i>password</i>—Password to use; it can include spaces if the character string is enclosed in quotation marks.• max-outstanding-requests <i>value</i>—Maximum number of outstanding requests in flight to server. Range: 1 through 65,335 files• source-address <i>source-address</i>—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.• timeout <i>seconds</i>—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

rapid-commit

Syntax rapid-commit;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcpv6-client]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Used to signal the use of the two-message exchange for address assignment.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [DHCPv6 Client Overview on page 1120](#)
- [Understanding DHCPv6 Client and Server Identification on page 1116](#)

reconfigure (System Services DHCP)

Syntax	<pre>reconfigure { attempts <i>number</i>; clear-on-abort; strict; timeout <i>number</i>; token <i>token-name</i>; trigger { radius-disconnect; } }</pre>
Hierarchy Level	<pre>[edit system services dhcp-local-server dhcpv6] [edit system services dhcp-local-server group <i>group-name</i>] [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]</pre>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.
Options	<p>attempts <i>number</i>—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.</p> <p>Range: 1 through 10 attempts</p> <p>Default: 8 attempts</p> <p>clear-on-abort—Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.</p> <p>strict—Configure the system to only allow packets that contain the reconfigure accept option.</p> <p>timeout <i>seconds</i>—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempts doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.</p> <p>Range: 1 through 10 seconds</p> <p>Default: 2 seconds</p> <p>token <i>token-name</i>—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).</p>

trigger — Specify DHCP reconfigure trigger.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 1088](#)
- [DHCP Server Configuration Overview on page 1092](#)

req-option

Syntax req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcpv6-client]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description The configuration options requested by the DHCPv6 client.

Options

dns-server—Specify a DNS server.

domain—Specify a domain name.

fqdn—Specify a fully qualified domain name.

nis-domain—Specify a Network Information Service (NIS) domain.

nis-server—Specify a Network Information Service (NIS) server.

ntp-server—Specify a Network Time Protocol (NTP) server.

sip-domain—Specify a Session Initiation Protocol (SIP) domain.

sip-server—Specify a Session Initiation Protocol (SIP) server.

time-zone—Specify a time zone.

vendor-spec—Specify vendor specification.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

retransmission-attempt (dhcp-client)

Syntax	retransmission-attempts <i>number</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.
Options	number —Number of attempts to retransmit the packet. Range: 0 through 6
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

retransmission-attempt (dhcpv6-client)

Syntax	retransmission-attempt <i>number</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.
Options	number —Number of retransmit attempts
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

retransmission-interval (dhcp-client)

Syntax	retransmission-interval <i>seconds</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the time between successive retransmission attempts.
Options	seconds —Number of seconds between successive retransmission attempts. Range: 4 through 64 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

root-authentication

Syntax	<pre>root-authentication { encrypted-password <i>password</i>; load-key-file <i>URL</i>; plain-text-password; ssh-dsa <i>public-key</i> { <from <i>pattern-list</i>>; } ssh-rsa <i>public-key</i> { <from <i>pattern-list</i>>; } }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify authentication information for the root login.
Options	<ul style="list-style-type: none">• encrypted-password <i>password</i>—Specify the encrypted authentication password. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.• plain-text-password—The CLI prompts you for a password encrypts it, and stores the encrypted version in its user database.• load-key-file <i>URL</i>—File URL containing one or more SSH keys.• ssh-dsa <i>public-key</i>—SSH DSA public key string.<ul style="list-style-type: none">• from <i>pattern-list</i>—Pattern list of allowed hosts.• ssh-rsa <i>public-key</i>—SSH RSA public key string.<ul style="list-style-type: none">• from <i>pattern-list</i>—Pattern list of allowed hosts.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

single-connection

Syntax	single-connection;
Hierarchy Level	[edit system accounting destination tacplus server <i>server-address</i>] [edit system tacplus-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Optimize the attempt to connect to a TACACS+ server. Junos OS maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

server (NTP)

Syntax	<code>server address <key key-number> <version value> <prefer>;</code>
Hierarchy Level	[edit system ntp]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>For NTP, configure the SRX Series device to operate in client mode with the remote system at the specified address. In this mode, the SRX Series device can be synchronized with the remote system, but the remote system can never be synchronized with the SRX Series device.</p> <p>If the NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the client is automatically stepped back into synchronization. If the offset between the NTP client and server exceeds the 1000-second threshold, the client still synchronizes with the server, but it also generates a system log message noting that the threshold was exceeded.</p>
Options	<p>address—Address of the remote system. You must specify an address, not a hostname.</p> <p>key key-number—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.</p> <p>Range: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as the preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version value—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248

server-address (dhcp-client)

Syntax	server address <i>ip-address</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify the preferred DHCP server address that is sent to DHCP clients.
Options	ip-address —DHCP server address.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax	source-address <i>source-address</i> <routing-instance <i>routing-instance-name</i> >;
Hierarchy Level	[edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system <i>ntp</i>], [edit system <i>radius-server</i> <i>server-address</i>], [edit system <i>syslog</i>], [edit system <i>tacplus-server</i> <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify a source address for each configured TACACS+ server, RADIUS server, or NTP server, or the source address to record in system log messages that are directed to a remote machine.
Options	source-address —A valid IP address configured on one of the SRX Series devices. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • ntp on page 1248

ssh-known-hosts

Syntax	<pre>ssh-known-hosts { fetch-from-server <i>server-name</i>; host <i>hostname</i> { dsa-key <i>dsa-key</i>; ecdsa-sha2-nistp256-key <i>ecdsa-sha2-nistp256-key</i>; ecdsa-sha2-nistp384-key <i>ecdsa-sha2-nistp384-key</i>; ecdsa-sha2-nistp521-key <i>ecdsa-sha2-nistp521-key</i>; rsa-key <i>rsa-key</i>; rsa1-key <i>rsa1-key</i>; } load-key-file <i>key-file</i>; }</pre>
Hierarchy Level	[edit security]
Release Information	Statement modified in Junos OS Release 8.5.
Description	Configure SSH support for known hosts and for administering SSH host key updates.
Options	<ul style="list-style-type: none">• fetch-from-server <i>server-name</i>—Retrieve SSH public host key information from a specified server.• load-key-file <i>key-file</i>—Import SSH host-key information from the specified <code>/var/tmp/ssh-known-hosts</code> file. <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit security ssh-known-hosts] Hierarchy Level on page 1164

static-subscribers

Syntax	<code>static-subscribers { disable; }</code>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Associate subscribers with statically configured interfaces, and provide dynamic service activation for these subscribers.
Options	disable —Disable the static subscribers process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

statistics-service

Syntax	<code>statistics-service { command <i>binary-file-path</i>; disable; }</code>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the Packet Forwarding Engine (PFE) statistics service management process.
Options	<ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to the binary process. • disable—Disable the Packet Forwarding Engine (PFE) statistics service management process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

subscriber-management

Syntax	subscriber-management { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the subscriber management process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the subscriber management process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

subscriber-management-helper

Syntax	subscriber-management-helper { command <i>binary-file-path</i> ; disable; failover (alternate-media other-routing-engine); }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the subscriber management helper process.
Options	<ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the subscriber management helper process.• failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.<ul style="list-style-type: none">• alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.• other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

system master password

Syntax	<pre>set system master-password plain-text-password Master password: *** Repeat master password: ***</pre>
Hierarchy Level	system
Release Information	Statement introduced in Junos OS Release 15.1X49-D50.
Description	Use to set a master password in a hidden configuration within the Junos OS configuration database.
Options	<p>set system master-password iteration-count—(Optional) The number of iterations to use for the PBKDF2 hash function. The range is 10 through 10000. Default value is 100. High iteration counts can impact system performance on systems with many secrets.</p> <p>set system master-password pseudorandom-function (hmac-sha1 hmac-sha2-256 hmac-sha2-512); default hmac-sha2-256—(Optional) Hash (prf) algorithm to be used for the PBKDF2 key derivation.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> request system decrypt password

tacplus

Syntax	<pre>tacplus { server <i>server-address</i> { port <i>port-number</i>; secret <i>password</i>; single-connection; source-address <i>source-address</i>; timeout <i>seconds</i>; } }</pre>
Hierarchy Level	[edit system accounting destination]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the TACACS+ accounting server.
Options	<ul style="list-style-type: none">• <i>server-address</i>—Specify the address of the TACACS+ authentication server.• <i>port number</i>—Configure the port number on which to contact the TACACS+ server.• <i>single-connection</i>—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.• <i>source-address address</i>—Configure a source address for each configured TACACS+ server.• <i>timeout seconds</i>—Configure the amount of time that the local device waits to receive a response from a TACACS+ server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring a TACACS+ Server for System Authentication on page 1019

tacplus-options

Syntax	<pre> tacplus-options { (exclude-cmd-attribute no-cmd-attribute-value); enhanced-accounting; service-name <i>service-name</i>; timestamp-and-timezone; } </pre>
Hierarchy Level	[edit system]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>no-cmd-attribute-value and exclude-cmd-attribute options introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p>timestamp-and-timezone option introduced in Junos OS Release 12.2.</p> <p>enhanced-accounting option introduced in Junos OS Release 14.1.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>
Description	Configure TACACS+ options for authentication and accounting.
Options	<p>enhanced-accounting—View the attribute values of a logged in user.</p> <p>exclude-cmd-attribute—Exclude the cmd attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>no-cmd-attribute-value—Set the cmd attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>service-name <i>service-name</i>—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.</p> <p>Default: junos-exec</p> <p>timestamp-and-timezone—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 1018 • <i>Configuring TACACS+ System Accounting</i> • <i>Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication</i> • <i>enhanced-accounting</i>

tacplus-server

Syntax	<code>tacplus-server server-address { port <i>port-number</i>; secret <i>password</i>; single-connection; source-address <i>source-address</i>; timeoutseconds; }</code>
Hierarchy Level	[edit system]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the TACACS+ server.

- Options**
- **server-address**—Address of the TACACS+ authentication server.



NOTE: Wildcard characters cannot be used in the TACACS server address or source address. This is because the TACACS server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

- **port**—Port number of TACACS+ authentication server.
- **secret**—Password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server. Password to use; can include spaces included in quotation marks.
- **single-connection**—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
- **source-address**—Source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. Configure a valid IP address on one of the device interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level.
- **timeout**—The amount of time that the local device waits to receive a response from a RADIUS or TACACS+ server. The timeout range is 1 through 90 seconds. The default is 3 seconds.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

- Related Documentation**
- [Example: Configuring a TACACS+ Server for System Authentication on page 1019](#)

traceoptions (Outbound SSH)

Syntax	<pre> traceoptions { file { filename ; files <i>number</i>; match <i>regular-expression</i>; size <i>maximum-file-size</i>; (world-readable no-world-readable); } flag <i>flag</i>; no-remote-trace; } </pre>
Hierarchy Level	[edit system services outbound-ssh]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Set the trace options.
Options	<ul style="list-style-type: none"> file—Configure the trace file information. <ul style="list-style-type: none"> filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced. files <i>number</i>—Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed to trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten. <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 files</p> <p>Default: 10 files</p> match <i>regular-expression</i>—Refine the output to include lines that contain the regular expression. size <i>maximum-file-size</i>—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Syntax: x K to specify KB, x m to specify MB, or x g to specify GB</p> <p>Range: 10 KB through 1 GB</p>

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
 - **all**—Trace all events.
 - **configuration**—Trace configuration events.
 - **connectivity**—Trace TCP connection handling.
- **no-remote-trace**—Disable remote tracing.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Displaying Log and Trace Files on page 1900
------------------------------	---

traceoptions (System Services DHCP)

Syntax	<pre> traceoptions { file { filename; files number; size maximum-file-size; (world-readable no-world-readable); } flag flag; no-remote-trace; } </pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server] [edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure extended DHCP local server tracing operations for DHCP processes.
Options	<ul style="list-style-type: none"> • file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named jdhcpd in the directory /var/log. If you include the file statement, you must specify a filename. • files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option. <p>Range: 2 through 1000 Default: 3 files</p> <ul style="list-style-type: none"> • match regular-expression—(Optional) Refine the output to include lines that contain the regular expression. • size maximum-file-size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option. <p>Syntax: xk to specify KB, xm to specify MB, or xg to specify GB Range: 10 KB through 1 GB Default: 128 KB</p> <ul style="list-style-type: none"> • world-readable—(Optional) Enable unrestricted file access. • no-world-readable—(Optional) Disable unrestricted file access. • flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags: <ul style="list-style-type: none"> • all—Trace all events.

- **database**—Trace database operations.
- **dhcpv6-general**—Trace operations for DHCPv6.
- **dhcpv6-io**—Trace input/output operations for DHCPv6.
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-rpd**—Trace routing protocol process operations.
- **dhcpv6-session-db**—Trace session database operations for DHCPv6.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **fwd**—Trace firewall process operations.
- **general**—Trace miscellaneous general operations.
- **ha**—Trace high-availability related operations.
- **interface**—Trace interface operations.
- **io**—Trace input/output operations.
- **packet**—Trace packet decoding operations.
- **packet- option**—Trace DHCP option decoding operations.
- **performance**—Trace DHCP performance measurement operations.
- **profile**—Trace DHCP profile operations.
- **rpd**—Trace routing protocol process operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace changes in statistics.
- **ui**—Trace changes in user interface operations.
- **no remote-trace**—Disable remote tracing.

Required Privilege Level trace—To view this statement in the configuration.
 trace-control—To add this statement to the configuration.

Related Documentation • [System Configuration Statement Hierarchy on page 1165](#)

trusted-key

Syntax	<code>trusted-key [<i>key-numbers</i>];</code>
Hierarchy Level	[edit system <i>ntp</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For NTP, configure the keys you are allowed to use when you configure the SRX Series device to synchronize its time with other systems on the network.
Options	key-numbers —One or more key numbers. Each key can be any 32-bit unsigned integer except 0.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• ntp on page 1248

uac-service

Syntax	<pre>uac-service { command <i>binary-file-path</i>; disable; failover (alternate-media other-routing-engine); }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the unified access control daemon process.
Options	<ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to the binary process. • disable—Disable the unified access control daemon process. • failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot. <ul style="list-style-type: none"> • alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly. • other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Firewall User Authentication Overview</i>

update-router-advertisement

Syntax	update-router-advertisement (interface <i>interface-name</i>);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Specify the interface used to delegate prefixes.
Options	interface <i>interface-name</i> —Interface on which to delegate prefixes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

update-server (dhcp-client)

Syntax	update-server;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Propagate DHCP options to a local DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

update-server (dhcpv6-client)

Syntax	update-server;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Propagate TCP/IP settings to the DHCPv6 server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

usb-control

Syntax	usb-control { command <i>binary-file-path</i> ; disable; }
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the universal serial bus (USB) supervise process.
Options	<ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to the binary process. • disable—Disable the universal serial bus (USB) supervise process.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

use-interface

Syntax	use-interface-description {logical device};
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	The description configured at the physical or logical interface level is used for client identification.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

user-id

Syntax	<code>user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i>};</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

vendor-id

Syntax	<code>vendor-id <i>vendor-id</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.
Options	vendor-id —Vendor class ID.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	

vpn (Forwarding Options)

Syntax	<code>vpn;</code>
Hierarchy Level	[edit forwarding-options helpers bootp]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	For Dynamic Host Configuration Protocol (DHCP) or BOOTP client request forwarding, enable virtual private network (VPN) encryption for a client request to pass through a VPN tunnel.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Server, Client, and Relay Agent Overview on page 1088

watchdog

Syntax	<pre>watchdog { disable; enable; timeout <i>value</i>; }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Enable or disable the watchdog timer when Junos OS encounters a problem.
Options	<ul style="list-style-type: none"> • disable—Disable the watchdog timer. • enable—Enable the watchdog timer. • timeout <i>value</i>—Specify amount of time to wait in seconds. Range: 1 through 3600 seconds.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

web-management

Syntax	<pre>web-management { disable; failover (alternate-media other-routing-engine); }</pre>
Hierarchy Level	[edit system processes]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the Web management process.
Options	<ul style="list-style-type: none">• disable—Disable the Web management process.• failover—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.<ul style="list-style-type: none">• alternate-media—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.• other-routing-engine—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

web-management (System Services)

```
Syntax  web-management {
        http {
            interfaces interface-names ;
            port port;
        }
        https {
            interfaces interface-names;
            local-certificate name;
            pki-local-certificate name;
            system-generated-certificate name;
            port port;
        }
        management url management url;
        session {
            idle-timeout minutes;
            session-limit number;
        }
        traceoptions {
            file {
                filename;
                files number;
                match regular-expression;
                size maximum-file-size;
                (no-world-readable | world-readable);
            }
            flag flag;
            level level;
            no-remote-trace;
        }
    }
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 9.0.
Support for **https** introduced for high-end SRX Series Services Gateways starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.

Description Configure settings for HTTP or HTTPS access. HTTP access allows management of the device using the J-Web interface. HTTPS access allows secure management of the device using the J-Web interface. With HTTPS access, communication is encrypted between your browser and the webserver for your device.

Options **control**—Disable the SBC process.

- **max-threads**—Maximum simultaneous threads to handle requests.
Range: 0 through 16

http—Configure HTTP.

- **interface [value]**—Interface value that accepts HTTP access.

- **port *number***—TCP port for incoming HTTP connections.

Range: 1 through 65,535

https—Configure HTTPS.

- **interface [*value*]**—Interface value that accept HTTP access.
- **port *number***—TCP port for incoming HTTP connections.

Range: 1 through 65,535

- **local-certificate**—X.509 certificate to use from the configuration.
- **pki-local-certificate**—X.509 certificate to use from the PKI local store.
- **system-generated-certificate**—X.509 certificate generated automatically by the system.

management url *management url*—URL path for Web management access.

session—Configure the Web-management session.

- **idle-timout *minutes***—Default timeout of Web-management sessions in minutes.
- **session-limit *number***—Maximum number of Web-management sessions to allow.

traceoptions—Set the trace options.

- **file**—Configure the trace file information.
 - *filename*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
 - **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size maximum file-size** option.

Range: 2 through 1000 files

Default: 10 files

- **match regular-expression**—Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Range: 10 KB through 1 GB

Default: 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files number** option.

- **(world-readable | no-world-readable)**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag flag**—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
 - **all**—Trace all areas.
 - **configuration**—Trace configuration.
 - **dynamic-vpn**—Trace dynamic VPN events.
 - **init**—Trace the daemon init process.
 - **mgd**—Trace MGD requests.
 - **webauth**—Trace Web authentication requests.
- **level level**—Specify the level of debugging output.
 - **all**—Match all levels.
 - **error**—Match error conditions.

- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.
- **no-remote-trace**—Disable remote tracing.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Firewall User Authentication Overview</i>• <i>Dynamic VPN Overview</i>

CHAPTER 57

Operational Commands

- clear dhcp client binding
- clear dhcp client statistics
- clear dhcp relay binding
- clear dhcp relay statistics
- clear dhcp server binding
- clear dhcp server statistics
- clear dhcpv6 client binding
- clear dhcpv6 client statistics
- clear dhcpv6 server binding (Local Server)
- clear dhcpv6 server statistics (Local Server)
- clear system login lockout
- file archive
- file checksum md5
- file checksum sha1
- file checksum sha-256
- file compare
- file copy
- file delete
- file list
- file rename
- file show
- request dhcp client renew
- request dhcpv6 client renew
- request system autorecovery state
- request system decrypt password
- request system download abort
- request system download clear
- request system download pause

- [request system download resume](#)
- [request system download start](#)
- [request system firmware upgrade](#)
- [request system license update](#)
- [request system power-off fpc](#)
- [request system services dhcp](#)
- [request system snapshot \(SRX Series\)](#)
- [request system software abort in-service-upgrade \(ICU\)](#)
- [request system software add \(Maintenance\)](#)
- [request system reboot](#)
- [request system software rollback \(SRX Series\)](#)
- [request system zeroize](#)
- [restart \(Reset\)](#)
- [Restart Commands Overview on page 1342](#)
- [show chassis routing-engine \(View\)](#)
- [show cli authorization](#)
- [show dhcp client binding](#)
- [show dhcp client statistics](#)
- [show dhcp relay binding](#)
- [show dhcp relay statistics](#)
- [show dhcp server binding](#)
- [show dhcp server statistics](#)
- [show dhcpv6 client binding](#)
- [show dhcpv6 client statistics](#)
- [show dhcpv6 server binding \(View\)](#)
- [show dhcpv6 server statistics \(View\)](#)
- [show firewall \(View\)](#)
- [show system autorecovery state](#)
- [show system download](#)
- [show system license \(View\)](#)
- [show system login logout](#)
- [show system services dhcp client](#)
- [show system services dhcp relay-statistics](#)
- [show system snapshot media](#)
- [show system storage partitions \(View SRX Series\)](#)

clear dhcp client binding

Syntax	clear dhcp client binding [all interface <interface-name>] [routing-instance <routing-instance-name>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.
Options	<p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>interface <interface-name>—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p>routing-instance <routing-instance-name>—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp client binding on page 1346
Output Fields	This command produces no output.

clear dhcp client statistics

Syntax	clear dhcp client statistics <all> <interface> <routing-instance>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.
Options	<p>all—(Optional) Clear all the DHCP client statistics.</p> <p>interface—(Optional) Clear the statistics for DHCP clients on the specified interface.</p> <p>routing-instance —(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp client statistics on page 1349
Output Fields	This command produces no output.

clear dhcp relay binding

Syntax	clear dhcp relay binding <all ip-address mac-address> <interface interface-name> <routing-instance routing-instance-name>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.
Options	<p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p>mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcp relay binding on page 1351
Output Fields	This command produces no output.

clear dhcp relay statistics

Syntax	clear dhcp relay statistics <routing-instance routing-instance-name>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	routing-instance routing-instance-name —(Optional) Clear the DHCP relay statistics on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp relay statistics on page 1353
Output Fields	This command produces no output.

clear dhcp server binding

Syntax	<code>clear dhcp server binding</code> <code><all ip-address mac-address></code> <code><interface interface-name></code> <code><routing-instance routing-instance-name></code>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.
Options	<p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p>mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp server binding on page 1355
Output Fields	This command produces no output.

clear dhcp server statistics

Syntax	clear dhcp server statistics <routing-instance routing-instance-name>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	routing-instance routing-instance-name —(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp server statistics on page 1357
Output Fields	This command produces no output.

clear dhcpv6 client binding

Syntax	clear dhcpv6 client binding [all interface <i>interface-name</i>] [routing-instance <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table.
Options	<p>all—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p>interface <i>interface-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for DHCPv6 clients on the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcpv6 client binding on page 1359
Output Fields	This command produces no output.

clear dhcpv6 client statistics

Syntax	clear dhcpv6 client statistics routing-instance <i>routing-instance-name</i>
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Clear all DHCPv6 client statistics.
Options	routing-instance <i>routing-instance-name</i> —(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcpv6 client statistics on page 1361
Output Fields	This command produces no output.

clear dhcpv6 server binding (Local Server)

Syntax	clear dhcpv6 server binding <all <i>client-id</i> <i>ip-address</i> <i>session-id</i> > <interface <i>interface-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 10.4.
Description	Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.
Options	<ul style="list-style-type: none"> • all—(Optional) Clear the binding state for all DHCPv6 clients. • <i>client-id</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1). • <i>ip-address</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified address. • <i>session-id</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID. • interface <i>interface-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified interface. • routing-instance <i>routing-instance-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcpv6 server binding (View) on page 1363

clear dhcpv6 server statistics (Local Server)

Syntax	<code>clear dhcpv6 server statistics</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Clear all DHCPv6 local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcpv6 server statistics (View) on page 1367

clear system login logout

Syntax	clear system login logout <all> <user <i>username</i> >
Release Information	Command introduced in Junos OS Release 11.2.
Description	Unlock the user account locked as a result of invalid login attempts.
Options	all —Clear all locked user accounts. user <i>username</i> —Clear the specified locked user account.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• lockout-period on page 1244• show system login logout on page 409
Output Fields	This command produces no output.

file archive

Syntax	<code>file archive destination <i>destination</i> source <i>source</i> <compress></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.
Options	<p>destination <i>destination</i>—Name of the created archive. Specify the destination as a URL or filename.</p> <p>source <i>source</i>— Path of directory to archive.</p> <p>compress—(Optional) Compress the archived file with the GNU zip (gzip) compression utility. The compressed files have the suffix .tgz.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i>
List of Sample Output	file archive (Multiple Files) on page 1302 file archive (Single File) on page 1302 file archive (with Compression) on page 1302
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file archive (Multiple Files)

The following sample command archives all message files in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive source /var/log/messages* destination /var/log/messages-archive.tar
/usr/bin/tar: Removing leading / from absolute path names in the archive.
```

file archive (Single File)

The following sample command archives one message file in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive source /var/log/messages destination /var/log/messages-archive.tar
/usr/bin/tar: Removing leading / from absolute path names in the archive.
user@host
```

file archive (with Compression)

The following sample command archives and compresses all message files in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive compress source /var/log/messages* destination  
/var/log/messages-archive.tgz  
/usr/bin/tar: Removing leading / from absolute path names in the archive.
```

file checksum md5

Syntax	<code>file checksum md5 <i>path</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Calculate the Message Digest 5 (MD5) checksum of a file.
Options	<i>path</i> —(Optional) Path to a filename.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>• file checksum sha1 on page 1305• file checksum sha-256 on page 1306
List of Sample Output	file checksum md5 on page 1304
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum md5

```
user@host> file checksum md5 jbundle-5.3R2.4-export-signed.tgz
MD5 (jbundle-5.3R2.4-export-signed.tgz) = 2a3b69e43f9bd4893729cc16f505a0f5
```


file checksum sha1

Syntax	<code>file checksum sha1 <i>path</i></code>
Release Information	Command introduced in Junos OS Release 9.5.
Description	Calculate the Secure Hash Algorithm (SHA-1) checksum of a file.
Options	<i>path</i> —(Optional) Path to a filename.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i> • file checksum md5 on page 1304 • file checksum sha-256 on page 1306
List of Sample Output	file checksum sha1 on page 1305
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha1

```
user@host> file checksum sha1 /var/db/scripts/opscript.slax
```

```
SHA1 (/var/db/scripts/commitscript.slax) = ba9e47120c7ce55cff29afd73eacd370e162c676
```

file checksum sha-256

Syntax	<code>file checksum sha-256 <i>path</i></code>
Release Information	Command introduced in Junos OS Release 9.5.
Description	Calculate the Secure Hash Algorithm 2 family (SHA-256) checksum of a file.
Options	<i>path</i> —(Optional) Path to a filename.
Required Privilege Level	maintenance view view-configuration
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>• file checksum sha1 on page 1305• file checksum md5 on page 1304
List of Sample Output	file checksum sha-256 on page 1306
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha-256

```
user@host> file checksum sha-256 /var/db/scripts/commitscript.slax

SHA256 (/var/db/scripts/commitscript.slax) =
94c2b061fb55399e15babd2529453815601a602b5c98e5c12ed929c9d343dd71
```

file compare

Syntax	<code>file compare (files <i>from-file to-file</i>) <context unified> <ignore-white-space></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	<p>Compare two local files and describe the differences between them in default, context, or unified output styles:</p> <ul style="list-style-type: none"> • default—In the first line of output, c means lines were changed between the two files, d means lines were deleted between the two files, and a means lines were added between the two files. The numbers preceding this alphabetical marker represent the first file, and the lines after the alphabetical marker represent the second file. A left angle bracket (<) in front of output lines refers to the first file. A right angle bracket (>) in front of output lines refers to the second file. • context—The display is divided into two parts. The first part is the first file; the second part is the second file. Output lines preceded by an exclamation point (!) have changed. Additions are marked with a plus sign (+), and deletions are marked with a minus sign (-). • unified—The display is preceded by the line number from the first and the second file (xx,xxx,x). Before the line number, additions to the file are marked with a plus sign (+), and deletions to the file are marked with a minus sign (-). The body of the output contains the affected lines. Changes are viewed as additions plus deletions.
Options	<p>files <i>from-file</i>—Names of files to compare.</p> <p>files <i>to-file</i>—Names of files to compare against.</p> <p>context—(Optional) Display output in context format.</p> <p>ignore-white-space—(Optional) Ignore changes in the amount of white space.</p> <p>unified—(Optional) Display output in unified format.</p>
Required Privilege Level	none
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i>
List of Sample Output	<p>file compare files on page 1308</p> <p>file compare files context on page 1308</p> <p>file compare files unified on page 1308</p> <p>file compare files unified ignore-white-space on page 1308</p>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file compare files

```
user@host> file compare files /tmp/one /tmp/two
100c100
<          full-name "File 1";
---
>          full-name "File 2";
102c102
<          class foo; # 'foo' is not defined
---
>          class super-user;
```

file compare files context

```
user@host> file compare files /tmp/one /tmp/two context
*** /tmp/one   Wed Dec  3 17:12:50 2003
--- /tmp/two   Wed Dec  3 09:13:14 2003
*****
*** 97,104 ****
        }
    }
    user bill {
!       full-name "Bill Smith";
!       class foo; # 'foo' is not defined
        authentication {
            encrypted-password SECRET;
        }
--- 97,105 ----
    }
    user bill {
!       full-name "Bill Smith";
!       uid 1089;
!       class super-user;
        authentication {
            encrypted-password SECRET;
        }
    }
```

file compare files unified

```
user@host> file compare files /tmp/one /tmp/two unified
--- /tmp/one   Wed Dec  3 17:12:50 2003
+++ /tmp/two   Wed Dec  3 09:13:14 2003
@@ -97,8 +97,9 @@
    }
}
user bill {
-   full-name "Bill Smith";
-   class foo; # 'foo' is not defined
+   full-name "Bill Smith";
+   uid 1089;
+   class super-user;
    authentication {
        encrypted-passwordSECRET;
    }
}
```

file compare files unified ignore-white-space

```
user@host> file compare files /tmp/one /tmp/two unified ignore-white-space
```

```
--- /tmp/one    Wed Dec  3 09:13:10 2003
+++ /tmp/two    Wed Dec  3 09:13:14 2003
@@ -99,7 +99,7 @@
     user bill {
         full-name "Bill Smith";
         uid 1089;
-        class foo; # 'foo' is not defined
+        class super-user;
         authentication {
             encrypted-password <SECRET>; # SECRET-DATA
         }
     }
```

file copy

Syntax `file copy source destination`
`<source-address source- address>`

Release Information Command introduced before Junos OS Release 7.4.

Description Copy files from one location to another location on the local device or to a location on a remote device that is reachable by the local device.



WARNING: The `sslv3-support` option is not available for configuration with the `set system services xnm-ssl` and `file copy` commands. SSLv3 is no longer supported or available.

You can use the `set system services xnm-ssl sslv3-support` command to enable SSLv3 for a Junos XML protocol client application to use as the protocol to connect to the Junos XML protocol server on a device, and you can use the `file copy source destination sslv3-support` command to enable the copying of files from an SSLv3 URL.

Using SSLv3 presents a potential security vulnerability, and we recommend that you not use SSLv3. For more details about this security vulnerability, go to <http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10656>.

Required Privilege Level maintenance

Related Documentation

- *Administration Guide for Security Devices*

List of Sample Output

- [Copy a File from the Local Device to a Personal Computer on page 1310](#)
- [Copy a Configuration File Between Routing Engines on page 1311](#)
- [Copy a Log File Between Routing Engines on page 1311](#)
- [Copy a File Using FTP on page 1311](#)
- [Copy a File Using FTP and Requiring a Password on page 1311](#)
- [Copy a File Using Secure Copy on page 1311](#)

Sample Output

The following are examples of a variety of file copy scenarios.

Copy a File from the Local Device to a Personal Computer

```
user@host> file copy /var/tmp/rpd.core.4 mypc:/c/junipero/tmp
```

```
...transferring.file..... | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
```

Copy a Configuration File Between Routing Engines

The following sample command copies a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

Copy a Log File Between Routing Engines

The following sample command copies a log file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy lcc0-re0:/var/log/chassisd lcc0-re1:/var/tmp
```

Copy a File Using FTP

To use anonymous FTP to copy a local file to a remote system:

```
user@host> file copy filename ftp://hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
user@host> file copy /config/juniper.conf ftp://hostname/juniper.conf
Receiving ftp: //hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using FTP and Requiring a Password

To use FTP where you require more privacy and are prompted for a password:

```
root@host> file copy filename ftp://user@hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
root@host> file copy /config/juniper.conf ftp://user@hostname/juniper.conf
Password for user@hostname: *****
Receiving ftp: //user@hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using Secure Copy

To use scp to copy a local file to a remote system:

```
root@host> file copy filename scp://user@hostname/path/filename
```

In the following example, `/config/juniper.conf` is the local file, `user` is the username, and `ssh-host` is the scp server:

```
root@host> file copy /config/juniper.conf scp://user@ssh-host/tmp/juniper.conf
user@ssh-host's password: *****
juniper.conf          100%
| ***** |
2198          00:00
```

file delete

Syntax	<code>file delete path</code> <code><purge></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Delete a path on the device.
Options	path —Name of the path to delete. purge —(Optional) Overwrite regular files before deleting them.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>
List of Sample Output	file delete on page 1312
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file delete

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file delete /var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpd.core
```


file list

Syntax	<code>file list path</code> <detail recursive>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display a list of paths on the device.
Options	<p>path—(Optional) Display a list of paths.</p> <p>detail recursive—(Optional) Display detailed output or descend recursively through the directory hierarchy, respectively.</p>
Additional Information	The default directory is the home directory of the user logged in to the device. To view available directories, enter a space and then a slash (/) after the file list command. To view files within a specific directory, include a slash followed by the directory and, optionally, subdirectory name after the file list command.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i>
List of Sample Output	file list on page 1313
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file list

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core
```

file rename

Syntax	<code>file rename <i>source destination</i></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Rename a file on the device.
Options	<i>destination</i> —New name for the file. <i>source</i> —Original name of the file.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i>
List of Sample Output	file rename on page 1314
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file rename

The following example lists the files in `/var/tmp`, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file rename /var/tmp/dcd.core /var/tmp/dcd.core.990413
user@host> file list /var/tmp
dcd.core.990413
rpd.core
snmpd.core
```

file show

Syntax	<code>file show <i>filename</i></code> <code><encoding (base64 raw)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the contents of a file.
Options	<p><i>filename</i>—Name of a file.</p> <p>encoding (base64 raw)—(Optional) Encode file contents with base64 encoding or show raw text.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i>
List of Sample Output	file show on page 1315
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

file show

```

user@host> file show /var/log/messages
Apr 13 21:00:08 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:00:40 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:02:48 romney last message repeated 4 times
Apr 13 21:07:04 romney last message repeated 8 times
Apr 13 21:07:13 romney /kernel: so-1/1/0: Clearing SONET alarm(s) RDI-P
Apr 13 21:07:29 romney /kernel: so-1/1/0: Asserting SONET alarm(s) RDI-P
...

```


request dhcp client renew

Syntax	<code>request dhcp client renew</code> <code>[all interface <interface-name>]</code> <code>routing-instance <routing-instance-name></code>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Initiates a renew request for the specified clients if they are in the bound state.
Options	<p>all—Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.</p> <p>interface <interface-name>—Initiate renew requests for DHCP clients on the specified interface.</p> <p>routing-instance <routing-instance-name>—Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• request dhcpv6 client renew on page 1317
Output Fields	This command produces no output.

request dhcpv6 client renew

Syntax	<code>request dhcpv6 client renew</code> <code>[all interface <i>interface-name</i>]</code> <code>routing-instance <<i>routing-instance-name</i>></code>
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Initiate a renew request for the specified DHCPv6 clients if they are in the bound state.
Options	<p>all—Initiate renew requests for all DHCPv6 clients. If you specify a routing instance, renew requests are initiated for all DHCPv6 clients within that routing instance.</p> <p>interface-name <i>interface-name</i>—Initiate renew requests for DHCPv6 clients on the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate renew requests for DHCPv6 clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.</p>
Required Privilege Level	view
Output Fields	This command produces no output.

request system autorecovery state

Syntax	request system autorecovery state (save recover clear)
Release Information	Command introduced in Junos OS Release 11.2.
Description	Prepare the system for autorecovery of configuration, licenses, and disk information.
Options	<p>save—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.</p> <p>The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.</p>
	<div>  <p>NOTE:</p> <ul style="list-style-type: none"> Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed. A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten. </div>
	<p>recover—Recover the disk partitioning, configuration, and licenses.</p> <p>After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.</p>
	<p>clear—Clear all saved autorecovery information.</p> <p>Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> show system autorecovery state on page 385
List of Sample Output	request system autorecovery state save on page 1319 request system autorecovery state recover on page 1319 request system autorecovery state clear on page 1319
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

`request system autorecovery state save`

```
user@host> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving bsdlablel recovery information
```

Sample Output

`request system autorecovery state recover`

```
user@host> request system autorecovery state recover

Configuration:
File           Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File           Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Saved                Failed           Recovered
BSD Labels:
Slice          Recovery Information  Integrity Check  Action / Status
s1             Saved                Passed           None
s2             Saved                Passed           None
s3             Saved                Passed           None
s4             Saved                Passed           None
```

Sample Output

`request system autorecovery state clear`

```
user@host> request system autorecovery state clear
Clearing config recovery information
Clearing license recovery information
Clearing bsdlablel recovery information
```

request system decrypt password

Syntax	request system decrypt password
Release Information	Statement introduced in Junos OS Release 15.1X49-D50.
Description	Use to display plain text versions of obfuscated (\$9) or encrypted (\$8) passwords. If the password was encrypted using the new \$8\$ method, you are prompted for the master password.
Options	<ul style="list-style-type: none">decrypt—Decrypt a \$8\$-encrypted or \$9\$-encrypted password.
Required Privilege Level	system
Output Fields	When you enter this command, you are provided feedback on the status of your request.


Sample Output

```
// Decrypting a $9 password
user@host> request system decrypt password $9$ABC123
Plaintext password: mysecret
```

Sample Output

```
// Decrypting a $8 password
user@host> request system decrypt password $8$ABC123
Master password:
Plaintext password: mysecret
(Simple passwords like "mysecret" are discouraged. This is an example only.)
```


request system download abort

Syntax	request system download abort <download-id>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the show system download command until a request system download clear operation is performed.
<div>  NOTE: Only downloads in the active, paused, and error states can be aborted. </div>	
Options	download-id —(Required) The ID number of the download to be aborted.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 298 • request system download pause on page 296 • request system download resume on page 297 • request system download clear on page 295
List of Sample Output	request system download abort on page 1321
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

request system download clear


Syntax	request system download clear
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Delete the history of completed and aborted downloads.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 298• request system download pause on page 296• request system download resume on page 297• request system download abort on page 294
List of Sample Output	request system download clear on page 1322
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause


Syntax	request system download pause <download-id>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Suspend a particular download instance.
<div>  NOTE: Only downloads in the active state can be paused. </div>	
Options	download-id —(Required) The ID number of the download to be paused.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 298 • request system download resume on page 297 • request system download abort on page 294 • request system download clear on page 295
List of Sample Output	request system download pause on page 1323
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```

request system download resume

Syntax	<code>request system download resume <i>download-id</i> <max-rate></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the request system download start command. The user can optionally specify a new (maximum) bandwidth with the request system download resume command.
<div>  NOTE: Only downloads in the paused and error states can be resumed. </div>	
Options	download-id —(Required) The ID number of the download to be resumed. max-rate —(Optional) The maximum bandwidth for the download.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 298 • request system download pause on page 296 • request system download abort on page 294 • request system download clear on page 295
List of Sample Output	request system download resume on page 1324
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

Syntax	<code>request system download start (url max-rate save as login delay)</code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Creates a new download instance and identifies it with a unique integer called the download ID.
Options	<p>url—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p>max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.</p> <p>save-as—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p>login—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p>delay—(Optional) The number of hours after which the download should start.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download pause on page 296 • request system download resume on page 297 • request system download abort on page 294 • request system download clear on page 295
List of Sample Output	request system download start on page 1325
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server/tftpboot/1m_file
max-rate 1k
Starting download #1
```

request system firmware upgrade

Syntax	request system firmware upgrade
Release Information	Command introduced in Junos OS Release 10.2.
Description	Upgrade firmware on a system.
Options	<p>fpc—Upgrade FPC ROM monitor.</p> <p>pic—Upgrade PIC firmware.</p> <p>re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p>vcpu—Upgrade VCPU ROM monitor.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> request system license update on page 305
List of Sample Output	request system firmware upgrade on page 1326
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```

user@host> request system firmware upgrade re bios
Part          Type          Tag Current  Available Status
              version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1  1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re bios backup
Part          Type          Tag Current  Available Status
              version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1  1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

```

request system license update

Syntax	<code>request system license update</code>
Release Information	Command introduced in Junos OS Release 9.5.
Description	Start autoupdating license keys from the LMS server.
Options	<code>trial</code> —Starts autoupdating trial license keys from the LMS server.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • show system license (View) on page 406
List of Sample Output	request system license update on page 1327 request system license update trial on page 1327
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system license update

```
user@host> request system license update
```

```
Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system power-off fpc

Syntax	request system (halt power-off reboot) power-off fpc
Release Information	Command introduced in Junos OS Release 11.4.
Description	Bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down.
Options	<ul style="list-style-type: none">• halt—Bring FPC offline and then halt the system.• power-off—Bring FPC offline and then power off the system.• reboot—Bring FPC offline and then reboot the system.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system reboot on page 1334
List of Sample Output	request system halt power-off fpc on page 1328 request system power-off power-off fpc on page 1328 request system reboot power-off fpc on page 1328
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system halt power-off fpc

```
user@host> request system halt power-off fpc
Halt the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system power-off power-off fpc

```
user@host> request system power-off power-off fpc
Power off the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system reboot power-off fpc

```
user@host> request system reboot power-off fpc
Reboot the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system services dhcp

Syntax	request system services dhcp (release <i>interface-name</i> renew <i>interface-name</i>)
Release Information	Command introduced in Junos OS Release 8.5.
Description	<p>Release or renew the acquired IP address for a specific interface.</p> <p>To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the show system services dhcp client <i>interface-name</i> command.</p>
Options	<ul style="list-style-type: none">• release <i>interface-name</i> —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.• renew <i>interface-name</i> —Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>dhcp</i>• show system services dhcp client on page 1380
Output Fields	This command produces no output.

request system snapshot (SRX Series)

Syntax request system snapshot
 <factory>
 <media (compact-flash | hard-disk | internal | usb)>
 <node (all | local | node-id | primary)>
 <partition>
 <slice (alternate) >

Release Information Command introduced in Junos OS Release 10.2.

Description Back up the currently running and active file system partitions on the device.

- Options**
- media— (Optional) Specifies the media to be included in the snapshot:
 - compact-flash— Copies the snapshot to the CompactFlash card.
 - hard-disk— Copies the snapshot to the hard disk.
 - usb— Copies the snapshot to the USB storage device.
 - node— (Optional) Specifies the archive data and executable areas of a specific node.
 - node-id— Specifies for node(0, 1).
 - all— Specifies for all nodes.
 - local— Specifies for local nodes.
 - primary— Specifies for primary nodes.
 - partition - (Default) Specifies that the target media should be repartitioned before the backup is saved to it.



NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

Example: **request system snapshot media usb partition**

Example: **request system snapshot media usb partition factory**

- slice— (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
- alternate— (Optional) Stores the snapshot on the other root partition in the system.



NOTE: The slice option cannot be used along with the other **request system snapshot** options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	request system snapshot media hard-disk on page 1331 request system snapshot media usb (when usb device is missing on page 1331 request system snapshot media compact-flash on page 1331 request system snapshot partition on page 1331
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

[request system snapshot media usb \(when usb device is missing](#)

```
user@host> request system snapshot media usb
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

[request system snapshot media compact-flash](#)

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

[request system snapshot partition](#)

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

request system software abort in-service-upgrade (ICU)

Syntax	request system software abort in-service-upgrade
Release Information	Command introduced in Junos OS Release 11.2.
Description	Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the request system in-service-upgrade command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>request system software in-service-upgrade (Maintenance)</i>
List of Sample Output	request system software abort in-service-upgrade on page 1332
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

request system software add (Maintenance)

Syntax	<code>request system software add <i>package-name</i></code>
Release Information	Partition option introduced in the command in Junos OS Release 10.1.
Description	Install the new software package on the device. For example: request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.
Options	<ul style="list-style-type: none">• <code>delay-restart</code> — Installs the software package but does not restart the software process• <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors• <code>no-copy</code> — Installs the software package but does not saves the copies of package files• <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts• <code>partition</code> — Formats and re-partitions the media before installation• <code>reboot</code> — Reboots the device after installation is completed• <code>unlink</code> — Removes the software package after successful installation• <code>validate</code> — Checks the compatibility with current configuration before installation starts
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system reboot on page 1334

request system reboot

Syntax `request system reboot <at time> <in minutes> <media> <message 'text'>`

Release Information Command introduced in Junos OS Release 10.1.
 Command **hypervisor** option introduced in Junos OS Release 15.1X49-D10 for vSRX.
 Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.

Description Reboot the software.

- Options**
- **at time**— Specifies the time at which to reboot the device . You can specify time in one of the following ways:
 - **now**— Reboots the device immediately. This is the default.
 - **+minutes**— Reboots the device in the number of minutes from now that you specify.
 - **yymmddhhmm**— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
 - **hh:mm**— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
 - **in minutes**— Specifies the number of minutes from now to reboot the device. This option is a synonym for the **at +minutes** option
 - **media type**— Specifies the boot device to boot the device from:
 - **disk/internal**— Reboots from the internal media. This is the default.
 - **usb**— Reboots from the USB storage device.
 - **compact flash**— Reboots from the external CompactFlash card.



NOTE: The **media** command option is not available on vSRX.

- **message text**— Provides a message to display to all system users before the device reboots.

Example: **request system reboot at 5 in 50 media internal message stop**

Required Privilege Level maintenance

Related Documentation • [request system software rollback \(SRX Series\) on page 356](#)

request system software rollback (SRX Series)

Syntax	request system software rollback <node-id>
Release Information	Command introduced in Junos OS Release 10.1. Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.
Description	Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback .
Options	<i>node-id</i> —Identification number of the chassis cluster node. It can be 0 or 1.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system reboot on page 1334

request system zeroize

Syntax `request system zeroize <media>`

Description Erases all configuration information and resets all key values. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories.

The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the Junos OS command-line interface (CLI) by typing `cli` at the prompt.

Options **media**—(Optional) In addition to removing all configuration and log files, the media option causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and the like. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the request system zeroize media operation can take considerably more time than the request system zeroize operation. However, the critical security parameters are all removed at the beginning of the process.



NOTE: The media option is not supported on SRX5000 line devices.

Required Privilege Level Not applicable.

Related Documentation

- [request system reboot on page 1334](#)
- [request system software rollback \(SRX Series\) on page 356](#)

List of Sample Output [request system zeroize on page 1336](#)

Sample Output

request system zeroize

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no)  yes

warning: zeroizing re0

Loading /boot/loader   Consoles: serial port
BIOS driver C: is disk0
```



```
BIOS 607kB/2087552kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.1
(builder@youcompany.com, Mon Mar 28 20:49:26 UTC 2011)
Loading /boot/defaults/loader.conf
/kernel text=0x837a60 data=0x46a78+0x9d44c syms=[0x4+0x8f38+0x4+0xca1ee]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
platform_early_bootinit: MAG Series Early Boot Initilaization
GDB: debug ports: sio
GDB: current port: sio
KDB: debugger backends: ddb gdb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights resrved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 18\989, 1991, 1992, 1993,1994
The Regents of the University of California. All rights reserved.
...
output truncated
```

restart (Reset)

Syntax restart
 <application-identification | application-security | audit-process | commitd-service
 | chassis-control | class-of-service | database-replication | datapath-trace-service | ddns
 | dhcp | dhcp-service | dynamic-flow-capture | disk-monitoring | event-processing |
 ethernet-connectivity-fault-management | ethernet-link-fault-management
 | extensible-subscriber-services | fipsd | firewall | firewall-authentication-service
 | general-authentication-service | gracefully | gprs-process | idp-policy | immediately
 | interface-control | ipmi | ipsec-key-management | jflow-service | jnu-management
 | jnx-wmicd-service | jsrp-service | kernel-replication | l2-learning | l2cpd-service | lacp
 | license-service | logical-system-service | mib-process | mountd-service | named-service
 | network-security | network-security-trace | nfsd-service | ntpd-service | pgm
 | pic-services-logging | profilerd | pki-service | remote-operations | rest-api | routing | sampling
 | sampling-route-record | scc-chassisd | secure-neighbor-discovery | security-intelligence
 | security-log | services | service-deployment | simple-mail-client-service | soft | snmp
 | static-routed | statistics-service | subscriber-management | subscriber-management-helper
 | system-log-vital | tunnel-oamd | uac-service | user-ad-authentication | vrrp
 | web-management >

Release Information Command introduced before Junos OS Release 9.2

Description Restart a Junos OS process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

- Options**
- application-identification—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
 - application-security—(Optional) Restart the application security process.
 - audit-process—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, for analyzing and tracking usage patterns, and for billing a user based upon the amount of time used or the type of services accessed.
 - chassis-control—(Optional) Restart the chassis management process.
 - class-of-service—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.
 - commitd-service—(Optional) Restart the committed services.
 - database-replication—(Optional) Restart the database replication process.
 - datapath-trace-service—(Optional) Restart the Restart the packet path tracing process.
 - ddns—(Optional) Restart the dynamic domain name system, which dynamically updates IP addresses for registered domain names.

- `dhcp`—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
- `dhcp-service`—(Optional) Restart the Dynamic Host Configuration Protocol process.
- `disk-monitoring`—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.
- `dynamic-flow-capture`—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on PIC3 monitoring services cards.
- `ethernet-connectivity-fault-management`—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.
- `ethernet-link-fault-management`—(Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.
- `event-processing`—(Optional) Restart the event process (`eventd`).
- `extensible-subscriber-services`—(Optional) Restart the extensible subscriber services process.
- `fipsd`—(Optional) Restart the `fipsd` services.
- `firewall`—(Optional) Restart the firewall management process, which manages the firewall configuration and accepts or rejects packets that are transiting an interface on a router or switch.
- `firewall-authentication-service`—(Optional) Restart the firewall authentication service process.
- `general-authentication-service`—(Optional) Restart the general authentication process.
- `gprs-process`—(Optional) Restart the General Packet Radio Service (GPRS) process.
- `gracefully`—(Optional) Restart the software process.
- `idp-policy`—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.
- `immediately`—(Optional) Immediately restart the software process.
- `interface-control`—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.
- `ipmi`—(Optional) Restart the intelligent platform management interface process.
- `ipsec-key-management`—(Optional) Restart the IPsec key management process.
- `jflow-service`—(Optional) Restart `jflow` service process.
- `jnu-management`—(Optional) Restart `jnu` management process.
- `jnx-wmicd-service`—(Optional) Restart `jnx wmicd` service process.
- `jsrp-service`—(Optional) Restart the Juniper Services Redundancy Protocol (`jsrdp`) process, which controls chassis clustering.

- **kernel-replication**—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.
- **lACP**—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link. The LACP process allows link aggregation control instances to reach agreement on the identity of the LAG to which a link belongs, moves the link to that LAG, and enables the transmission and reception processes for the link to function in an orderly manner.
- **l2cpd-service**—(High-end SRX Series only) (Optional) Restart the Layer 2 Control Protocol (L2CP) process, which enables features such as L2 protocol tunneling and nonstop bridging.
- **l2-learning**—(Optional) Restart the Layer 2 (L2) address flooding and learning process.
- **license-service**—(Optional) Restart the feature license management process.
- **logical-system-service**—(Optional) Restart the logical system service process.
- **mib-process**—(Optional) Restart the MIB version II process, which provides the router's MIB II agent.
- **mountd-service**—(Optional) Restart the service for Network File System (NFS) mount requests.
- **named-service**—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.
- **network-security**—(Optional) Restart the network security process.
- **network-security-trace**—(Optional) Restart the network security trace process.
- **nfsd-service**—(Optional) Restart the remote NFS server process, which provides remote file access for applications that need NFS-based transport.
- **ntpd-service**—(Optional) Restart the Network Time Protocol (NTP) process.
- **pgm**—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.
- **pic-services-logging**—(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.
- **pki-service**—(Optional) Restart the public key infrastructure (PKI) service process.
- **profillerd**—(Optional) Restart the profiler process.
- **remote-operations**—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
- **rest-api**—(Optional) Restart the rest api process.
- **routing**—(Optional) Restart the routing protocol process (rpd).
- **sampling**—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.

- `sampling-route-record`—(Optional) Restart the sampling route record process.
- `scc-chassisd`—(Optional) Restart the scc chassisd process.
- `secure-neighbor-discovery`—(Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.
- `security-intelligence`—(Optional) Restart security intelligence process.
- `security-log`—(Optional) Restart the security log process.
- `service-deployment`—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.
- `services`—(Optional) Restart a service.
- `simple-mail-client-service`—(Optional) Restart the simple mail client service process.
- `snmp`—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.
- `static-routed`—(Optional) Restart the static routed process.
- `soft`—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.
- `statistics-service`—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.
- `subscriber-management`—(Optional) Restart the subscriber management process.
- `subscriber-management-helper`—(Optional) Restart the subscriber management helper process.
- `system-log-vital`—(Optional) Restart system log vital process.
- `tunnel-oamd`—(Optional) Restart the tunnel OAM process for L2 tunneled networks.
- `uac-service`—(Optional) Restart the Unified Access Control (UAC) process.
- `user-ad-authentication`—(Optional) Restart User ad Authentication process
- `vrrp`—(Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.
- `web-management`—(Optional) Restart the Web management process.

Required Privilege Level reset

Related Documentation • [Restart Commands Overview on page 1342](#)

List of Sample Output [restart interfaces on page 1342](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

Restart Commands Overview

Use the **restart** operational commands to restart software processes on the device. Operational commands are organized alphabetically.

Related Documentation

- [restart on page 740](#)

show chassis routing-engine (View)

Syntax	show chassis routing-engine
Release Information	Command introduced in Junos OS Release 9.5.
Description	Display the Routing Engine status of the chassis cluster.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • cluster (Chassis) on page 1998 • request system snapshot (SRX Series) on page 331
List of Sample Output	show chassis routing-engine (Sample 1 - SRX550M) on page 1344 show chassis routing-engine (Sample 2- vSRX) on page 1344
Output Fields	Table 90 lists the output fields for the show chassis routing-engine command. Output fields are listed in the approximate order in which they appear.

Table 90: show chassis routing-engine Output Fields

Field Name	Field Description
Temperature	Routing Engine temperature. (Not available for vSRX deployments.)
CPU temperature	CPU temperature. (Not available for vSRX deployments.)
Total memory	Total memory available on the system.
Control plane memory	Memory available for the control plane.
Data plane memory	Memory reserved for data plane processing.
CPU utilization	Current CPU utilization statistics on the control plane core.
User	Current CPU utilization in user mode on the control plane core.
Background	Current CPU utilization in nice mode on the control plane core.
Kernel	Current CPU utilization in kernel mode on the control plane core.
Interrupt	Current CPU utilization in interrupt mode on the control plane core.
Idle	Current CPU utilization in idle mode on the control plane core.
Model	Routing Engine model.
Start time	Routing Engine start time.

Table 90: show chassis routing-engine Output Fields (*continued*)

Field Name	Field Description
Uptime	Length of time the Routing Engine has been up (running) since the last start.
Last reboot reason	Reason for the last reboot of the Routing Engine.
Load averages	The average number of threads waiting in the run queue or currently executing over 1-, 5-, and 15-minute periods.

Sample Output

show chassis routing-engine (Sample 1 - SRX550M)

```

user@host> show chassis routing-engine
Routing Engine status:
  Temperature          38 degrees C / 100 degrees F
  CPU temperature      36 degrees C / 96 degrees F
  Total memory         512 MB Max  435 MB used ( 85 percent)
    Control plane memory 344 MB Max  296 MB used ( 86 percent)
    Data plane memory   168 MB Max  138 MB used ( 82 percent)
  CPU utilization:
    User                8 percent
    Background          0 percent
    Kernel              4 percent
    Interrupt           0 percent
    Idle                88 percent
  Model                RE-SRX5500-LOWMEM
  Serial ID            AAP8652
  Start time           2009-09-21 00:04:54 PDT
  Uptime               52 minutes, 47 seconds
  Last reboot reason    0x200:chassis control reset
  Load averages:       1 minute   5 minute   15 minute
                       0.12       0.15       0.10

```

Sample Output

show chassis routing-engine (Sample 2- vSRX)

```

user@host> show chassis routing-engine
Routing Engine status:
  Total memory         1024 MB Max  358 MB used ( 35 percent)
  Control plane memory 1024 MB Max  358 MB used ( 35 percent)
  5 sec CPU utilization:
    User                2 percent
    Background          0 percent
    Kernel              4 percent
    Interrupt           6 percent
    Idle                88 percent
  Model                VSRX RE
  Start time           2015-03-03 07:04:18 UTC
  Uptime               2 days, 11 hours, 51 minutes, 11 seconds
  Last reboot reason    Router rebooted after a normal shutdown.
  Load averages:       1 minute   5 minute   15 minute
                       0.07       0.04       0.06

```


show cli authorization

Syntax show cli authorization

Release Information Command introduced before Junos OS Release 7.4.

Description Display the permissions for the current user.

```
user@host> show cli authorization
Current user: 'root' login: 'boojum' class '(root)'
Permissions:
Permissions:
  admin          -- Can view user accounts
  admin-control-- Can modify user accounts
  clear          -- Can clear learned network info
  configure      -- Can enter configuration mode
  control        -- Can modify any config
  edit          -- Can edit full files
  field          -- Can use field debug commands
  floppy         -- Can read and write the floppy
  interface      -- Can view interface configuration
  interface-control-- Can modify interface configuration
  network        -- Can access the network
  reset          -- Can reset/restart interfaces and daemons
  routing        -- Can view routing configuration
  routing-control-- Can modify routing configuration
  shell          -- Can start a local shell
  snmp           -- Can view SNMP configuration
  snmp-control-- Can modify SNMP configuration
  system         -- Can view system configuration
  system-control-- Can modify system configuration
  trace          -- Can view trace file settings
  trace-control-- Can modify trace file settings
  view           -- Can view current values and statistics
  maintenance    -- Can become the super-user
  firewall       -- Can view firewall configuration
  firewall-control-- Can modify firewall configuration
  secret         -- Can view secret statements
  secret-control-- Can modify secret statements
  rollback       -- Can rollback to previous configurations
  security       -- Can view security configuration
  security-control-- Can modify security configuration
  access         -- Can view access configuration
  access-control-- Can modify access configuration
  view-configuration-- Can view all configuration (not including secrets)
  flow-tap       -- Can view flow-tap configuration
  flow-tap-control-- Can modify flow-tap configuration
  idp-profiler-operation-- Can Profiler data
  pgcp-session-mirroring-- Can view pgcp session mirroring configuration
  pgcp-session-mirroring-control-- Can modify pgcp session mirroring configuration
  storage        -- Can view fibre channel storage protocol configuration
  storage-control-- Can modify fibre channel storage protocol configuration
  all-control    -- Can modify any configuration
```

Required Privilege Level view

show dhcp client binding

Syntax	show dhcp client binding [<address> interface <interface-name>] routing-instance <routing-instance name> [brief detail summary]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.
Options	<p>address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:</p> <ul style="list-style-type: none"> ip-address—The specified IP address. mac-address—The specified MAC address. <p>routing-instance <routing-instance name>—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.</p> <p>interface <interface-name>—(Optional) Perform this operation on the specified interface.</p> <p>brief—(Optional) Display brief information about the active client bindings.</p> <p>detail—(Optional) Display detailed client binding information.</p> <p>summary—(Optional) Display a summary of DHCP client information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcp client binding on page 1291
List of Sample Output	show dhcp client binding on page 1347
Output Fields	Table 91 lists the output fields for the show dhcp client binding command. Output fields are listed in the approximate order in which they appear.

Table 91: show dhcp client binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Server	IP address of the DHCP server.
Expires	Number of seconds in which the lease expires.

Table 91: show dhcp client binding Output Fields (*continued*)

Field Name	Field Description
State	State of the address binding table on the DHCP local server.
Interface	Interface on which the request was received.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds in which the lease expires.
Lease Start	Date and time at which the client's IP address lease started.
Vendor Identifier	Vendor identifier.
Server Identifier	IP address of the DHCP server.
Client IP Address	IP address of the DHCP client.

Sample Output

show dhcp client binding

```

user@host> show dhcp client binding
2 clients, (2 bound, 0 init, 0 discover, 0 renew, 0 rebind)

      IP address      Hardware address      Server      Expires      State
Interface
  10.1.1.89           00:0a:12:00:12:12      10.1.1.1      348          BOUND
fe-0/0/1.0
  20.1.1.90           00:0a:12:00:12:34      20.1.1.1      568          BOUND
fe-0/0/2.0

user@host> show dhcp client binding interface fe-0/0/1.0 detail
Client Interface: fe-0/0/1.0
      Hardware address:      00:0a:12:00:12:12
      State:                  BOUND
      Lease Expires:          2010-09-16 14:45:41 UTC
      Lease Expires in:       528 seconds
      Lease Start:            2010-09-16 14:35:41 UTC
      Vendor Identifier:       ether
      Server Identifier:       10.1.1.1
      Client IP Address:       10.1.1.89
      update server            enabled

      DHCP Options :
      Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3
]
      Name: server-identifier, Value: 10.1.1.1
      Name: router, Value: [ 10.1.1.80 ]
      Name: domain-name, Value: example-50

user@host> show dhcp client binding 10.1.1.89
IP address      Hardware address      Server      Expires      State      Interface

```

10.1.1.89	00:0a:12:00:12:12	10.1.1.1	348	BOUND
fe-0/0/1.0				

show dhcp client statistics

Syntax	show dhcp client statistics <routing-instance <i>routing-instance-name</i> >
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display Dynamic Host Configuration Protocol (DHCP) client statistics.
Options	routing-instance <i>routing-instance-name</i> —(Optional) Display the statistics for DHCP clients on the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcp client statistics on page 1292
List of Sample Output	show dhcp client statistics on page 1350
Output Fields	Table 92 lists the output fields for the show dhcp client statistics command. Output fields are listed in the approximate order in which they appear.

Table 92: show dhcp client statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.
Messages received	Number of DHCP messages received. <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP protocol data units (PDUs) received • DHCPOFFER—Number of DHCP PDUs of type OFFER received • DHCPACK—Number of DHCP PDUs of type ACK received • DHCPNACK—Number of DHCP PDUs of type NACK received • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received

Table 92: show dhcp client statistics (*continued*)

Field Name	Field Description
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted • DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted • DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted • DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted • DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted • DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted • DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted

Sample Output

show dhcp client statistics

```

user@host> show dhcp client statistics
Packets dropped:
    Total                0
Messages received:
    BOOTREPLY            0
    DHCPOFFER            0
    DHCPACK              0
    DHCPNAK              0
    DHCPFORCERENEW      0
Messages sent:
    BOOTREQUEST          0
    DHCPDECLINE          0
    DHCPDISCOVER         0
    DHCPREQUEST          0
    DHCPINFORM           0
    DHCPRELEASE          0
    DHCPRENEW            0
    DHCPREBIND           0

```

show dhcp relay binding

Syntax	Show dhcp relay binding [<address> interface <interface-name>] routing-instance <routing-instance name> [brief detail summary]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.
Options	<p>address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:</p> <ul style="list-style-type: none"> ip-address—The specified IP address. mac-address—The specified MAC address. <p>routing-instance <routing-instance name>—(Optional) Display DHCP binding information on the specified routing instance.</p> <p>interface <interface-name>—(Optional) Perform this operation on the specified interface.</p> <p>brief—(Optional) Display brief information about the active client bindings.</p> <p>detail—(Optional) Display detailed client binding information.</p> <p>summary—(Optional) Display a summary of DHCP client information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcp relay binding on page 1293
List of Sample Output	show dhcp relay binding on page 1352
Output Fields	Table 93 lists the output fields for the show dhcp relay binding command. Output fields are listed in the approximate order in which they appear.

Table 93: show dhcp relay binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.

Table 93: show dhcp relay binding Output Fields (*continued*)

Field Name	Field Description
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp relay binding

```

user@host> show dhcp relay binding detail
IP address      Hardware address  Type      Lease expires      State
100.20.32.1     90:00:00:01:00:01 active    2007-01-17 11:38:47 PST
rebind
100.20.32.3     90:00:00:02:00:01 active    2007-01-17 11:38:41 PST
rebind
100.20.32.4     90:00:00:03:00:01 active    2007-01-17 11:38:01 PST
rebind
100.20.32.5     90:00:00:04:00:01 active    2007-01-17 11:38:07 PST
rebind
100.20.32.6     90:00:00:05:00:01 active    2007-01-17 11:38:47 PST
rebind

```

```

user@host> show dhcp relay binding 100.20.32.1
Active binding information:
    IP address      100.20.32.1
    Hardware address 90:00:00:01:00:01

Lease information:
    Type            DHCP
    Obtained at     2007-01-17 11:28:47 PST
    Expires at      2007-01-17 11:38:47 PST

> show dhcp relay binding 100.20.32.1 detail
Active binding information:
    IP address      100.20.32.1
    Hardware address 90:00:00:01:00:01
    Request received on fe-0/0/2.0, relayed by 100.20.32.2

Lease information:
    Type            DHCP
    Obtained at     2007-01-17 11:28:47 PST
    Expires at      2007-01-17 11:38:47 PST
    State           rebind

```


show dhcp relay statistics

Syntax	show dhcp relay statistics [<routing-instance>]
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	routing-instance —(Optional) Display the DHCP relay statistics on the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcp relay statistics on page 1294
List of Sample Output	show dhcp relay statistics on page 1353
Output Fields	Table 94 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear.

Table 94: show dhcp relay statistics

Field Name	Field Description
Messages received	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received DHCPDECLINE—Number of DHCP PDUs of type DECLINE received DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received DHCPREQUEST—Number of DHCP PDUs of type REQUEST received DHCPINFORM—Number of DHCP PDUs of type INFORM received DHCPRELEASE—Number of DHCP PDUs of type RELEASE received
Messages sent	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> BOOTREPLY—Number of BOOTP PDUs transmitted DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted DHCPACK—Number of DHCP PDUs of type ACK transmitted DHCPNACK—Number of DHCP PDUs of type NACK transmitted DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show dhcp relay statistics

```

user@host> show dhcp relay statistics
Messages received:
    BOOTREQUEST          0
    DHCPDECLINE          0
  
```

DHCPDISCOVER	0
DHCPINFORM	0
DHCPRELEASE	0
DHCPREQUEST	0
Messages sent:	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0
DHCPFORCERENEW	0

show dhcp server binding

Syntax	show dhcp server binding [interface <interface name>] <brief detail summary verbose> <ip-address MAC address> <routing-instance routing-instance-name>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.
Options	<p>interface <interface name>—(Optional) Display information about active client bindings on the specified interface.</p> <p>brief detail summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcp server binding.</p> <p>ip-address—Display DHCP binding information for a specific client identified by the specified IP address.</p> <p>MAC address—Display DHCP binding information for a specific client identified by the specified MAC address.</p> <p>routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcp server binding on page 1295
List of Sample Output	show dhcp server binding on page 1356
Output Fields	Table 95 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.

Table 95: show dhcp server binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.

Table 95: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp server binding

```
user@host> show dhcp server binding 100.20.32.1 detail
Active binding information:
    IP address          100.20.32.1
    Hardware address    90:00:00:01:00:01
    Request received on fe-0/0/2.0, relayed by 100.20.32.2

Lease information:
    Type                DHCP
    Obtained at         2007-01-17 11:28:47 PST
    Expires at          2007-01-17 11:38:47 PST
    State               rebind
```

show dhcp server statistics

Syntax	show dhcp server statistics <routing-instance>
Release Information	Statement introduced in Junos OS Release 12.1X44-D10.
Description	Display Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	routing-instance —(Optional) Display information about DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp server statistics on page 1296
List of Sample Output	show dhcp server statistics on page 1358
Output Fields	Table 96 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.

Table 96: show dhcp server statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.
Messages received	Number of DHCP messages sent. <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received
Messages sent	Number of DHCP messages received. <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show dhcp server statistics

```
user@host> show dhcp server statistics
Packets dropped:
  Total                                0

Messages received:
  BOOTREQUEST                         0
  DHCPDECLINE                         0
  DHCPDISCOVER                        0
  DHCPINFORM                          0
  DHCPRELEASE                         0
  DHCPREQUEST                         0

Messages sent:
  BOOTREPLY                           0
  DHCPOFFER                           0
  DHCPACK                             0
  DHCPNAK                             0
  DHCPFORCERENEW                      0
```

show dhcpv6 client binding

Syntax	show dhcpv6 client binding interface <i>interface-name</i> routing-instance < <i>routing-instance-name</i> > [brief detail summary]
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.
Options	<p>interface <i>interface-name</i>—(Optional) Perform this operation on the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.</p> <p>brief—(Optional) Display brief information about the active client bindings.</p> <p>detail—(Optional) Display detailed client binding information.</p> <p>summary—(Optional) Display a summary of DHCPv6 client information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcpv6 client binding on page 1297
List of Sample Output	show dhcpv6 client binding on page 1360
Output Fields	Table 97 lists the output fields for the show dhcpv6 client binding command. Output fields are listed in the approximate order in which they appear.

Table 97: show dhcpv6 client binding Output Fields

Field Name	Field Description
Hardware Address	Hardware address of the DHCPv6 client.
State	State of the address-binding table on the DHCPv6 local server.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds until the lease expires.
Lease Start	Date and time at which the client's IP address lease started.
Client DUID	The DHCPv6 client's unique identifier.
Bind type	The bind type.

Table 97: show dhcpv6 client binding Output Fields (*continued*)

Field Name	Field Description
Client Type	The type of DHCPv6 client. The client type can be autoconfig or stateful.
Rapid Commit	Two-message exchange option for address assignment.
Server IP Address	IP address of the DHCPv6 server.
Client IP Address	IP address of the DHCPv6 client.

Sample Output

show dhcpv6 client binding

```

user@host> show dhcpv6 client binding
IP prefix      Expires      ClientType  State  Interface      Client DUID
2001:db8::b2b7:8631:d968:8d5e/128 96          STATEFUL    BOUND ge-0/0/1.0
LL_TIME0x3-0x0-2c:6b:f5:62:39:c1

```

show dhcpv6 client binding detail

```

Client Interface: ge-0/0/1.0
  Hardware Address:      2c:6b:f5:62:39:c1
  State:                  BOUND(DHCPV6_CLIENT_STATE_BOUND)
  Lease Expires:         2012-08-07 15:52:19 UTC
  Lease Expires in:      116 seconds
  Lease Start:           2012-08-07 15:50:19 UTC
  Client DUID             VENDOR0x00000583-0x3000103f
  Bind Type:              IA_NA
  ClientType :            STATEFUL
  Rapid Commit            Off
  Server Ip Address:      fe80::230:48ff:fe5d:5bf7
  Client IP Address:      2001:db8::655b:3c80:2deb:1a3/128

DHCP options:
Name: server-identifier, Value: LL_TIME0x1-0x17acddab-00:30:48:5d:5b:f7
Name: vendor-opts, Value: 000005830002aaaa
Name: sip-server-list, Value: 2000::300 2000::302 2000::303 2000::304
Name: dns-recursive-server, Value: 2000::ff2000::fe
Name: domain-search-list, Value: 076578616d706c6503636f6d00

```


show dhcpv6 client statistics

Syntax	show dhcpv6 client statistics routing-instance<routing-instance-name>
Release Information	Statement introduced in Junos OS Release 12.1X45-D10.
Description	Display Dynamic Host Configuration Protocol (DHCPv6) client statistics.
Options	routing-instance <routing-instance-name> —(Optional) Display the statistics for DHCPv6 clients on the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 client statistics on page 1298
List of Sample Output	show dhcpv6 client statistics on page 1362
Output Fields	Table 98 lists the output fields for the show dhcpv6 client statistics command. Output fields are listed in the approximate order in which they appear.

Table 98: show dhcpv6 client statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the DHCPv6 Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE transmitted • DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT transmitted • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted • DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE transmitted • DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST transmitted • DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM transmitted • DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW transmitted • DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND transmitted

Table 98: show dhcpv6 client statistics Output Fields (*continued*)

Field Name	Field Description
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> DHCPV6_ADVERTISE—Number of DHCPv6 PDUs of type ADVERTISE received DHCPV6_REPLY—Number of DHCPv6 PDUs of type REPLY received DHCPV6_RECONFIGURE—Number of DHCPv6 PDUs of type RECONFIGURE received

Sample Output

show dhcpv6 client statistics

```

user@host> show dhcpv6 client statistics
Dhcpv6 Packets dropped:
    Total                0

Messages sent:
    DHCPV6_DECLINE        0
    DHCPV6_SOLICIT        3
    DHCPV6_INFORMATION_REQUEST 6
    DHCPV6_RELEASE        1
    DHCPV6_REQUEST        2
    DHCPV6_CONFIRM        0
    DHCPV6_RENEW          0
    DHCPV6_REBIND         0

Messages received:
    DHCPV6_ADVERTISE      3
    DHCPV6_REPLY          3
    DHCPV6_RECONFIGURE    0

```

show dhcpv6 server binding (View)

Syntax	show dhcpv6 server binding <brief detail summary> <interface <i>interface-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display the address bindings in the client table for DHCPv6 local server.
Options	<ul style="list-style-type: none"> • brief detail summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcpv6 server binding. • interface <i>interface-name</i>—(Optional) Display information about active client bindings on the specified interface. • routing-instance <i>routing-instance-name</i>—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 server binding (Local Server) on page 1299
List of Sample Output	show dhcpv6 server binding on page 1364 show dhcpv6 server binding detail on page 1365 show dhcpv6 server binding interface on page 1365 show dhcpv6 server binding interface detail on page 1365 show dhcpv6 server binding prefix on page 1366 show dhcpv6 server binding session-id on page 1366 show dhcpv6 server binding summary on page 1366
Output Fields	Table 99 lists the output fields for the show dhcpv6 server binding command. Output fields are listed in the approximate order in which they appear.

Table 99: show dhcv6p server binding Output Fields

Field Name	Field Description	Level of Output
<i>number</i> clients, (<i>number</i> init, <i>number</i> bound, <i>number</i> selecting, <i>number</i> requesting, <i>number</i> renewing, <i>number</i> releasing)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Prefix	Client's DHCPv6 prefix.	brief detail

Table 99: show dhc6p server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which lease expires.	brief detail
State	State of the address binding table on the DHCPv6 local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • INIT—Initial state. • RELEASE—Client is releasing IP address lease. • RECONFIGURE—Client has received reconfigure message from server. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCPv6 server. • SELECTING—Client receiving offers from DHCPv6 servers. 	brief detail
Interface	Interface on which the DHCPv6 request was received.	brief
Client DUID	Client's DHCP Unique Identifier (DUID).	brief detail
Lease expires	Date and time at which the client's IP address lease expires.	detail
Lease expires in	Number of seconds in which lease expires.	detail
Lease Start	Date and time at which the client's address lease was obtained.	detail
Incoming Client Interface	Client's incoming interface.	detail
Server IP Address	IP address of DHCPv6 server.	detail
Server Interface	Interface of DHCPv6 server.	detail
Client Id length	Length of the DHCPv6 client ID, in bytes.	detail
Client Id	ID of the DHCPv6 client.	detail

Sample Output

show dhc6p server binding

```
user@host> show dhc6p server binding
```

```

Prefix          Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 6      86321   BOUND   ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
```

```

2001:bd8:1111:2222::/64 7          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10         86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05

```

show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
```

```

Session Id: 6
  Client IPv6 Prefix:          2001:bd8:1111:2222::/64
  Client DUID:                  LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

  State:                        BOUND(bound)
  Lease Expires:                 2009-07-21 10:41:15 PDT
  Lease Expires in:              86308 seconds
  Lease Start:                   2009-07-20 10:41:15 PDT
  Incoming Client Interface:     ge-1/0/0.0
  Server Ip Address:             0.0.0.0
  Server Interface:              none
  Client Id Length:              14
  Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001

```

```

Session Id: 7
  Client IPv6 Prefix:          2001:bd8:1111:2222::/64
  Client DUID:                  LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:                        BOUND(bound)
  Lease Expires:                 2009-07-21 10:41:15 PDT
  Lease Expires in:              86308 seconds
  Lease Start:                   2009-07-20 10:41:15 PDT
  Incoming Client Interface:     ge-1/0/0.0
  Server Ip Address:             0.0.0.0
  Server Interface:              none
  Client Id Length:              14
  Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding interface

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
Prefix          Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 1      86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01

```

show dhcpv6 server binding interface detail

```
user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
```

```

Session Id: 7
  Client IPv6 Prefix:          2001:bd8:1111:2222::/64
  Client DUID:                  LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:                        BOUND(bound)
  Lease Expires:                 2009-07-21 10:41:15 PDT
  Lease Expires in:              86136 seconds
  Lease Start:                   2009-07-20 10:41:15 PDT
  Incoming Client Interface:     ge-1/0/0.0
  Server Ip Address:             0.0.0.0

```

```
Server Interface:          none
Client Id Length:         14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding prefix

```
user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id: 7
Client IPv6 Prefix:      2001:bd8:1111:2222::/64
Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

State:                   BOUND(bound)
Lease Expires:           2009-07-21 10:41:15 PDT
Lease Expires in:       86136 seconds
Lease Start:            2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:       0.0.0.0
Server Interface:        none
Client Id Length:        14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding session-id

```
user@host> show dhcpv6 server binding 8
Prefix      Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 8      86235 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

show dhcpv6 server statistics (View)

Syntax	show dhcpv6 server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display DHCPv6 local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 server statistics (Local Server) on page 1300
List of Sample Output	show dhcpv6 server statistics on page 1369
Output Fields	Table 100 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.

Table 100: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	<p>Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the DHCPv6 local server • Strict Reconfigure—Number of solicit messages discarded because the client does not support reconfiguration • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Invalid server address—Number of packets discarded because an invalid server address was specified • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the DHCPv6 local server could not send
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> • DHCPV6_CONFIRM—Number of DHCPv6 CONFIRM PDUs received. • DHCPV6_DECLINE—Number of DHCPv6 DECLINE PDUs received. • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • DHCPV6_REBIND—Number of DHCPv6 REBIND PDUs received. • DHCPV6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the DHCPv6 server. • DHCPV6_RELEASE—Number of DHCPv6 RELEASE PDUs received. • DHCPV6_RENEW—Number of DHCPv6 RENEW PDUs received. • DHCPV6_REQUEST—Number of DHCPv6 REQUEST PDUs received. • DHCPV6_SOLICIT—Number of DHCPv6 SOLICIT PDUs received.
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_REPLY—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted. • DHCPV6_RELAY_REPL—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
  Total          0

Messages received:
  DHCPV6_DECLINE          0
  DHCPV6_SOLICIT          9
  DHCPV6_INFORMATION_REQUEST 0
  DHCPV6_RELEASE          0
  DHCPV6_REQUEST          5
  DHCPV6_CONFIRM          0
  DHCPV6_RENEW            0
  DHCPV6_REBIND           0
  DHCPV6_RELAY_FORW       0
Messages sent:
  DHCPV6_ADVERTISE        9
  DHCPV6_REPLY             5
  DHCPV6_RECONFIGURE       0
  DHCPV6_RELAY_REPL        0
```

show firewall (View)

Syntax	<pre>show firewall <filter <i>filter-name</i>> <counter <i>counter-name</i>> <log> <prefix-action-stats> <terse></pre>
Release Information	Command introduced before Junos OS Release 10.0 .
Description	Display statistics about configured firewall filters.
Options	<p>none—Display statistics about configured firewall filters.</p> <p>filter <i>filter-name</i>—Name of a configured filter.</p> <p>counter <i>counter-name</i>—Name of a filter counter.</p> <p>log—Display log entries for firewall filters.</p> <p>prefix-action-stats—Display prefix action statistics for firewall filters.</p> <p>terse—Display firewall filter names only.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> firewall on page 896
List of Sample Output	show firewall on page 1371
Output Fields	Table 101 lists the output fields for the show firewall command. Output fields are listed in the approximate order in which they appear.

Table 101: show firewall Output Fields

Field Name	Field Description
Filter	<p>Name of a filter that has been configured with the filter statement at the [edit firewall] hierarchy level.</p> <p>When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either -i for an input filter or -o for an output filter.</p> <p>When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either -in for an input filter or -out for an output filter. When a logical system-specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, __ls1/filter1).</p>

Table 101: show firewall Output Fields (*continued*)

Field Name	Field Description
Counters	Display filter counter information: <ul style="list-style-type: none"> • Name—Name of a filter counter that has been configured with the counter firewall filter action. • Bytes—Number of bytes that match the filter term under which the counter action is specified. • Packets—Number of packets that matched the filter term under which the counter action is specified.
Policers	Display policer information: <ul style="list-style-type: none"> • Name—Name of policer. • Bytes—Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer. • Packets—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

Sample Output

show firewall

```

user@host> show firewall
Filter: ef_path
Counters:
Name          Bytes          Packets
def-count     0              0
video-count   0              0
voice-count    0              0

Filter: __default_bpdu_filter__

Filter: deep
Counters:
Name          Bytes          Packets
deep2         302076         5031

Filter: deep-flood
Counters:
Name          Bytes          Packets
deep_flood_def 302136         5032
deep1         0              0
Policers:
Name          Packets
deep-pol-op-first 0

```

show system autorecovery state

Syntax	show system autorecovery state
Release Information	Command introduced in Junos OS Release 11.2.
Description	Perform checks and show status of all autorecovered items.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system autorecovery state on page 292 • Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 169
List of Sample Output	show system autorecovery state on page 1372
Output Fields	Table 48 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear.

Table 102: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state
```

```
Configuration:
File          Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File          Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Not Saved           Not checked     Requires save
BSD Labels:
Slice         Recovery Information  Integrity Check  Action / Status
s1            Saved                Passed           None
s2            Saved                Passed           None
```

s3
s4

Saved
Saved

Passed
Passed

None
None

show system download

Syntax	<code>show system download <download-id></code>
Release Information	Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Display a brief summary of all the download instances along with their current state and extent of progress. If a download-id is provided, the command displays a detailed report of the particular download instance.
Options	<ul style="list-style-type: none"> download-id—(Optional) The ID number of the download instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> request system download start on page 298 Understanding Download Manager for SRX Series Devices on page 51 Understanding Download Manager for EX Series Devices
List of Sample Output	show system download on page 1374 show system download 1 on page 1375
Output Fields	Table 50 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear.

Table 103: show system download Output Fields

Field Name	Field Description
ID	Displays the download identification number.
Status	Displays the state of a particular download.
Start Time	Displays the start time of a particular download.
Progress	Displays the percentage of a download that has been completed.
URL	Displays the URL from which the file was downloaded.

Sample Output

show system download

```

user@host> show system download
Download Status Information:
ID  Status  Start Time      Progress  URL
1   Active   May 4 06:28:36  5%        ftp://ftp-server//tftpboot/1m_file
2   Active   May 4 06:29:07  3%        ftp://ftp-server//tftpboot/5m_file
3   Error    May 4 06:29:22  Unknown   ftp://ftp-server//tftpboot/badfile

```

4 Completed May 4 06:29:40 100% ftp://ftp-server//tftpboot/smallfile

show system download 1

```
user@host> show system download 1
```

```
Download ID      : 1
Status           : Active
Progress         : 6%
URL              : ftp://ftp-server//tftpboot/1m_file
Local Path       : /var/tmp/1m_file
Maximum Rate     : 1k
Creation Time    : May 4 06:28:36
Scheduled Time   : May 4 06:28:36
Start Time       : May 4 06:28:37
Error Count      : 0
```

show system license (View)

Syntax	show system license <installed keys status usage>
Release Information	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
Description	Display licenses and information about how licenses are used.
Options	<p>none—Display all license information.</p> <p>installed—(Optional) Display installed licenses only.</p> <p>keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p>status—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p>usage—(Optional) Display the state of licensed features.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Working with License Keys for SRX Series Devices</i>
List of Sample Output	<p>show system license on page 1377</p> <p>show system license installed on page 1377</p> <p>show system license keys on page 1378</p> <p>show system license usage on page 1378</p> <p>show system license status logical-system all on page 1378</p>
Output Fields	Table 52 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 104: show system license Output Fields

Field Name	Field Description
Feature name	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
Licenses used	Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.

Table 104: show system license Output Fields (*continued*)

Field Name	Field Description
Licenses installed	Information about the installed license key: <ul style="list-style-type: none"> • License identifier—Identifier associated with a license key. • License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • Valid for device—Device that can use a license key. • Features—Feature associated with a license.
Licenses needed	Number of licenses required for features being used but not yet properly licensed.
Expiry	Time remaining in the grace period before a license is required for a feature being used.
Logical system license status	Displays whether a license is enabled for a logical system.

Sample Output

show system license

```
user@host> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

```
Licenses installed:
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxxx xxxxxx xxx
```

show system license usage

```
user@host> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine 01:00:00 IST	1	1	0	2012-03-30
wf_key_surfcontrol_cpa 01:00:00 IST	0	1	0	2012-03-30
dynamic-vpn	0	1	0	permanent
ax411-wlan-ap	0	2	0	permanent

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:
```

logical system name	license status
root-logical-system	enabled
LSYS0	enabled
LSYS1	enabled
LSYS2	enabled

show system login logout

Syntax	show system login logout
Release Information	Command introduced in Junos OS Release 11.2.
Description	Display the usernames locked after unsuccessful login attempts.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> • lockout-period on page 1244 • clear system login logout on page 291
List of Sample Output	show system login logout on page 1379
Output Fields	Table 53 lists the output fields for the show system login logout command. Output fields are listed in the approximate order in which they appear.

Table 105: show system login logout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

Sample Output

show system login logout

```
user@host> show system login logout
```

```
User          Lockout start      Lockout end
root          2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC
```

show system services dhcp client

Syntax	<code>show system services dhcp client</code> <code>< interface-name ></code> <code><statistics></code>
Release Information	Command introduced in Junos OS Release 8.5. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display information about DHCP clients.
Options	<ul style="list-style-type: none"> • <code>none</code>—Display DHCP information for all interfaces. • <code>interface-name</code>—(Optional) Display DHCP information for the specified interface. • <code>statistics</code>—(Optional) Display DHCP client statistics.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> • <i>dhcp (Interfaces)</i> • request system services dhcp on page 1329 • <i>Administration Guide for Security Devices</i>
List of Sample Output	show system services dhcp client on page 1381 show system services dhcp client ge-0/0/34.0 on page 1382 show system services dhcp client statistics on page 1382
Output Fields	<p>Table 106 lists the output fields for the <code>show system services dhcp client</code> command. Output fields are listed in the approximate order in which they appear.</p>

Table 106: show system services dhcp client Output Fields

Field Name	Field Description
Logical Interface Name	Name of the logical interface.
Client Status	State of the client binding.
Vendor Identifier	Vendor ID.
Server Address	IP address of the DHCP server.
Address obtained	IP address obtained from the DHCP server.
Lease Obtained at	Date and time the lease was obtained.
Lease Expires in	(EX Series switches only) Time the current lease expires in (seconds).
<i>Reviewer: Madhavi, does this field exist in SRX platform as well?</i>	

Table 106: show system services dhcp client Output Fields (*continued*)

Field Name	Field Description
Lease Expires at	Date and time the lease expires.
DHCP Options	<ul style="list-style-type: none"> • Name: server-identifier, Value: IP address of the name server. • Name: device, Value: IP address of the name device. • Name: domain-name, Value: Name of the domain.
Packets dropped	Total packets dropped.
Messages received	<p>Number of the following DHCP messages received:</p> <ul style="list-style-type: none"> • DHCPOFFER—First packet received on a logical interface when DHCP is enabled. • DHCPACK—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stops the earlier timer added for DHCPACK. • DHCPNAK—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.
Messages sent	<p>Number of the following DHCP messages sent:</p> <ul style="list-style-type: none"> • DHCPDECLINE—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet. • DHCPDISCOVER—Packet sent on the interface for which the DHCP client is enabled. • DHCPREQUEST—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer. • DHCPINFORM—Packet sent to the DHCP server for local configuration parameters. • DHCPRELEASE—Packet sent to the DHCP server to relinquish network address and cancel remaining lease. • DHCPRENEW—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server. • DHCPREBIND—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.

Sample Output

show system services dhcp client

```

user@host> show system services dhcp client
Logical Interface name      ge-0/0/34.0
Hardware address           00:1f:12:38:5f:e5
Client status              bound
Address obtained           10.0.0.2
Update server              disabled
Lease obtained at          2013-12-23 08:11:40 UTC
Lease expires in           93
Lease expires at           2013-12-23 08:13:20 UTC

DHCP options:
  Name: server-identifier, Value: 10.0.0.1
  Code: 1, Type: ip-address, Value: 255.255.255.0

```

Sample Output

show system services dhcp client ge-0/0/34.0

```
user@host> show system services dhcp client ge-0/0/34.0
Logical Interface name      ge-0/0/34.0
Hardware address           00:1f:12:38:5f:e5
Client status               bound
Address obtained            10.0.0.2
Update server               disabled
Lease obtained at           2013-12-23 08:11:40 UTC
Lease expires in            87
Lease expires at            2013-12-23 08:13:20 UTC

DHCP options:
Name: server-identifier, Value: 10.0.0.1
Code: 1, Type: ip-address, Value: 255.255.255.0
```

Sample Output

show system services dhcp client statistics

```
user@host> show system services dhcp client statistics
Packets dropped:
  Total                      0
Messages received:
  DHCPPOFFER                  0
  DHCPACK                     8
  DHCPNAK                     0
Messages sent:
  DHCPDECLINE                  0
  DHCPDISCOVER                 0
  DHCPREQUEST                  1
  DHCPINFORM                   0
  DHCPRELEASE                  0
  DHCPRENEW                     7
  DHCPREBIND                   0
```

show system services dhcp relay-statistics

Syntax	<code>show system services dhcp relay-statistics</code>
Release Information	Command introduced in Junos OS Release 8.5 .
Description	Display information about the DHCP relay.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> <i>dhcp</i>
List of Sample Output	show system services dhcp relay-statistics on page 1383
Output Fields	Table 107 lists the output fields for the <code>show system services dhcp relay-statistics</code> command. Output fields are listed in the approximate order in which they appear.

Table 107: show system services dhcp relay-statistics Output Fields

Field Name	Field Description
Received packets	Total DHCP packets received.
Forwarded packets	Total DHCP packet forwarded.
Dropped packets	<p>Total DHCP packets dropped for the following reasons:</p> <ul style="list-style-type: none"> • Due to a missing interface in the relay database—Number of packets discarded because they did not belong to a configured interface. • Due to a missing matching routing instance—Number of packets discarded because they did not belong to a configured routing instance. • Due to an error during packet read—Number of packets discarded because of a system read error. • Due to an error during packet send—Number of packets that the DHCP relay application could not send. • Due to an invalid server address—Number of packets discarded because an invalid server address was specified. • Due to a missing valid local address—Number of packets discarded because there was no valid local address. • Due to a missing route to the server or client—Number of packets discarded because there were no addresses available for assignment.

Sample Output

show system services dhcp relay-statistics

```

user@host> show system services dhcp relay-statistics
Received packets: 4
Forwarded packets: 4
Dropped packets: 4
  Due to missing interface in relay database: 4
  Due to missing matching routing instance: 0

```

Due to an error during packet read: 0
Due to an error during packet send: 0
Due to invalid server address: 0
Due to missing valid local address: 0
Due to missing route to server/client: 0

show system snapshot media

Syntax	<code>show system snapshot media <i>media-type</i></code>
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Display the snapshot information for both root partitions on SRX Series devices
Options	<ul style="list-style-type: none"> • <code>internal</code>— Show snapshot information from internal media. • <code>usb</code>— Show snapshot information from device connected to USB port. • <code>external</code>— Show snapshot information from the external CompactFlash card.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 166
List of Sample Output	show system snapshot media internal on page 1385 show system snapshot media usb on page 1385

Sample Output

show system snapshot media internal

```
show system snapshot media internal
Information for snapshot on      internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos   : 10.1B3-domestic
Information for snapshot on      internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos   : 10.2-20100112.0-domestic
```

show system snapshot media usb

```
show system snapshot media usb
Information for snapshot on      usb (/dev/dals1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/dals2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```

show system storage partitions (View SRX Series)

Syntax	show system storage partitions
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Display the partitioning scheme details on SRX Series devices.
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 110
List of Sample Output	show system storage partitions (single root partitioning) on page 1386 show system storage partitions (USB) on page 1386

show system storage partitions (dual root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)
```

```
Partitions Information:
Partition Size Mountpoint
s1a 293M altroot
s2a 293M /
s3e 24M /config
s3f 342M /var
s4a 30M recovery
```

show system storage partitions (single root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Partitions Information:
Partition Size Mountpoint
s1a 898M /
s1e 24M /config
s1f 61M /var
```

show system storage partitions (USB)

```
show system storage partitions
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)
```

```
Partitions Information:
Partition Size Mountpoint
s1a 293M /
s2a 293M altroot
s3e 24M /config
```

s3f	342M	/var
s4a	30M	recovery

Network Management Administration Guide for Routing Devices

PART 16

Overview

- [Network Management Overview on page 1393](#)
- [Introduction to Network Monitoring on page 1397](#)

Network Management Overview

- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Understanding the Integrated Local Management Interface on page 1396](#)

Understanding Device Management Functions in Junos OS

After you have installed a device into your network, you need to manage the device within your network. Device management can be divided into five tasks:

- Fault management—Monitor the device; detect and fix faults.
- Configuration management—Configure device attributes.
- Accounting management—Collect statistics for accounting purposes.
- Performance management—Monitor and adjust device performance.
- Security management—Control device access and authenticate users.

The Junos[®] operating system (Junos OS) network management features work in conjunction with an operations support system (OSS) to manage the devices within the network. Junos OS can assist you in performing these management tasks, as described in [Table 108](#).

Table 108: Device Management Features in Junos OS

Task	Junos OS Feature
Fault management	<p>Monitor and see faults using:</p> <ul style="list-style-type: none"> Operational mode commands—For more information about operational mode commands, see the CLI Explorer, CLI Explorer, and CLI Explorer. SNMP MIBs—For more information about SNMP MIBs supported by Junos OS, see ““Standard SNMP MIBs Supported by Junos OS” on page 1409” and ““Enterprise-Specific SNMP MIBs Supported by Junos OS” on page 1427” in the <i>SNMP MIBs and Traps Reference</i> . Standard SNMP traps—For more information about standard SNMP traps, see the ““Standard SNMP Traps Supported on Devices Running Junos OS” on page 1456” in the <i>SNMP MIBs and Traps Reference</i> . Enterprise-specific SNMP traps—For more information about enterprise-specific traps, see ““Juniper Networks Enterprise-Specific SNMP Traps” on page 1456” in the <i>SNMP MIBs and Traps Reference</i> . System log messages—For more information about how to configure system log messages, see the <i>Junos OS Administration Library for Routing Devices</i>. For more information about how to view system log messages, see the System Log Explorer.
Configuration management	<ul style="list-style-type: none"> Configure router attributes using the command-line interface (CLI), the Junos XML management protocol, and the NETCONF XML management protocol. For more information about configuring the router using the CLI, see the <i>Junos OS Administration Library for Routing Devices</i>. For more information about configuring the router using the APIs, see the <i>Junos XML Management Protocol Guide</i> and <i>NETCONF XML Management Protocol Guide</i>. Configuration Management MIB—For more information about the Configuration Management MIB, see the “Configuration Management MIB” in the <i>SNMP MIBs and Traps Reference</i> .

Table 108: Device Management Features in Junos OS (*continued*)

Task	Junos OS Feature
Accounting management	<p>Perform the following accounting-related tasks:</p> <ul style="list-style-type: none"> Collect statistics for interfaces, firewall filters, destination classes, source classes, and the Routing Engine. For more information about collecting statistics, see “Accounting Options Configuration” on page 1678. Use interface-specific traffic statistics and other counters, available in the Standard Interfaces MIB, Juniper Networks enterprise-specific extensions to the Interfaces MIB, and media-specific MIBs, such as the enterprise-specific ATM MIB. Use per-ATM virtual circuit (VC) counters, available in the enterprise-specific ATM MIB. For more information about the ATM MIB, see the <i>SNMP MIBs and Traps Reference</i>. Group source and destination prefixes into source classes and destination classes and count packets for those classes. Collect destination class and source class usage statistics. For more information about classes, see <i>“Destination Class Usage MIB”</i> and <i>“Source Class Usage MIB”</i> in the <i>SNMP MIBs and Traps Reference</i>, “Configuring Class Usage Profiles” on page 1695, the <i>Junos OS Network Interfaces Library for Routing Devices</i>, and the <i>Junos OS Routing Protocols Library for Routing Devices</i>. Count packets as part of a firewall filter. For more information about firewall filter policies, see “Enterprise-Specific SNMP MIBs Supported by Junos OS” on page 1427 in the <i>SNMP MIBs and Traps Reference</i> and the <i>Junos OS Routing Protocols Library for Routing Devices</i>. Sample traffic, collect the samples, and send the collection to a host running the CAIDA cflowd utility. For more information about CAIDA and cflowd, see the <i>Junos OS Routing Protocols Library for Security Devices</i>.
Performance management	<p>Monitor performance in the following ways:</p> <ul style="list-style-type: none"> Use operational mode commands. For more information about monitoring performance using operational mode commands, see the CLI Explorer. Use firewall filter. For more information about performance monitoring using firewall filters, see the <i>Junos OS Routing Protocols Library for Routing Devices</i>. Sample traffic, collect the samples, and send the samples to a host running the CAIDA cflowd utility. For more information about CAIDA and cflowd, see the <i>Junos OS Routing Protocols Library for Routing Devices</i>. Use the enterprise-specific Class-of-Service MIB. For more information about this MIB, see the <i>“Class-of-Service MIB”</i> in the <i>SNMP MIBs and Traps Reference</i>.

Table 108: Device Management Features in Junos OS (*continued*)

Task	Junos OS Feature
Security management	<p>Assure security in your network in the following ways:</p> <ul style="list-style-type: none"> Control access to the router and authenticate users. For more information about access control and user authentication, see the <i>Junos OS Administration Library for Routing Devices</i>. Control access to the router using SNMPv3 and SNMP over IPv6. For more information, see “Configuring the Local Engine ID” on page 1506 and “Tracing SNMP Activity on a Device Running Junos OS” on page 1585.

- Related Documentation**
- [Understanding the Integrated Local Management Interface on page 1396](#)
 - [Understanding the SNMP Implementation in Junos OS](#)
 - [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)
 - [Accounting Options Overview on page 1673](#)

Understanding the Integrated Local Management Interface

The Integrated Local Management Interface (ILMI) provides a mechanism for Asynchronous Transfer Mode (ATM)-attached devices, such as hosts, routers, and ATM switches, to transfer management information. ILMI provides bidirectional exchange of management information between two ATM interfaces across a physical connection. ILMI information is exchanged over a direct encapsulation of SNMP version 1 (RFC 1157, *A Simple Network Management Protocol*) over ATM Adaptation Layer 5 (AAL5) using a virtual path identifier/virtual channel identifier (VPI/VCI) value (VPI=0, VCI=16).

Junos OS supports only two ILMI MIB variables: **atmfMYIPNmAddress** and **atmfPortMyIfname**. For ATM1 and ATM2 intelligent queuing (IQ) interfaces, you can configure ILMI to communicate directly with an attached ATM switch to enable querying of the switch's IP address and port number.

For more information about the ILMI MIB, see the ATM Forum at <http://www.atmforum.com/>.

- Related Documentation**
- [Understanding Device Management Functions in Junos OS](#)

Introduction to Network Monitoring

- [Monitoring Overview on page 1397](#)
- [Diagnostic Tools Overview on page 1398](#)

Monitoring Overview

Junos OS supports a suite of J-Web tools and CLI operational mode commands for monitoring the system health and performance of your device. Monitoring tools and commands display the current state of the device. To use the J-Web user interface and CLI operational tools, you must have the appropriate access privileges.

You can use the J-Web Monitor option to monitor a device. J-Web results appear in the browser.

You can also monitor the device with CLI operational mode commands. CLI command output appears on the screen of your console or management device, or you can filter the output to a file. For operational commands that display output, such as the **show** commands, you can redirect the output into a filter or a file. When you display help about these commands, one of the options listed is **|**, called a *pipe*, which allows you to filter the command output.

For example, if you enter the **show configuration** command, the complete device configuration appears on the screen. To limit the display to only those lines of the configuration that contain **address**, enter the **show configuration** command using a pipe into the **match** filter:

```
user@host> show configuration | match address
address-range low 192.168.3.2 high 192.168.3.254;
address-range low 192.168.71.71 high 192.168.71.254;
address 192.168.71.70/21;
address 192.168.2.1/24;
address 127.0.0.1/32;
```

For a complete list of the filters, type a command, followed by the pipe, followed by a question mark (?):

```
user@host> show configuration | ?
Possible completions:
compare          Compare configuration changes with prior version
count           Count occurrences
display         Show additional kinds of information
except          Show only text that does not match a pattern
```

find	Search for first occurrence of pattern
hold	Hold text without exiting the prompt
last	Display end of output only
match	Show only text that matches a pattern
no-more	Don't paginate output
request	Make system-level requests
resolve	Resolve IP addresses
save	Save output text to file
trim	Trim specified number of columns from start of line

You can specify complex expressions as an option for the **match** and **except** filters.



NOTE: To filter the output of configuration mode commands, use the filter commands provided for the operational mode commands. In configuration mode, an additional filter is supported.

- Related Documentation**
- [Monitoring Interfaces on page 1794](#)
 - [Diagnostic Tools Overview on page 1398](#)

Diagnostic Tools Overview

Juniper Networks devices support a suite of J-Web tools and CLI operational mode commands for evaluating system health and performance. Diagnostic tools and commands test the connectivity and reachability of hosts in the network.

- Use the J-Web Diagnose options to diagnose a device. J-Web results appear in the browser.
- Use CLI operational mode commands to diagnose a device. CLI command output appears on the screen of your console or management device, or you can filter the output to a file.

To use the J-Web user interface and CLI operational tools, you must have the appropriate access privileges.

This section contains the following topics:

- [J-Web Diagnostic Tools on page 1398](#)
- [CLI Diagnostic Commands on page 1399](#)

J-Web Diagnostic Tools

The J-Web diagnostic tools consist of the options that appear when you select **Troubleshoot** and **Maintain** in the task bar. [Table 109](#) describes the functions of the Troubleshoot options.

Table 109: J-Web Interface Troubleshoot Options

Option	Function
Troubleshoot Options	

Table 109: J-Web Interface Troubleshoot Options (*continued*)

Option	Function
Ping Host	Allows you to ping a remote host. You can configure advanced options for the ping operation.
Ping MPLS	Allows you to ping an MPLS endpoint using various options.
Traceroute	Allows you to trace a route between the device and a remote host. You can configure advanced options for the traceroute operation.
Packet Capture	Allows you to capture and analyze router control traffic.
Maintain Options	
Files	Allows you to manage log, temporary, and core files on the device.
Upgrade	Allows you to upgrade and manage Junos OS packages.
Licenses	Displays a summary of the licenses needed and used for each feature that requires a license. Allows you to add licenses.
Reboot	Allows you to reboot the device at a specified time.

CLI Diagnostic Commands

The CLI commands available in operational mode allow you to perform the same monitoring, troubleshooting, and management tasks you can perform with the J-Web user interface. Instead of invoking the tools through a graphical interface, you use operational mode commands to perform the tasks.

You can perform certain tasks only through the CLI. For example, you can use the **mtrace** command to display trace information about a multicast path from a source to a receiver, which is a feature available only through the CLI.

To view a list of top-level operational mode commands, type a question mark (?) at the command-line prompt.

At the top level of operational mode are the broad groups of CLI diagnostic commands listed in [Table 110](#).

Table 110: CLI Diagnostic Command Summary

Command	Function
Controlling the CLI Environment	
set option	Configures the CLI display.
Diagnosis and Troubleshooting	
clear	Clears statistics and protocol database information.
mtrace	Traces information about multicast paths from source to receiver.

Table 110: CLI Diagnostic Command Summary (*continued*)

Command	Function
monitor	Performs real-time debugging of various Junos OS components, including the routing protocols and interfaces.
ping	Determines the reachability of a remote network host.
ping mpls	Determines the reachability of an MPLS endpoint using various options.
test	Tests the configuration and application of policy filters and AS path regular expressions.
traceroute	Traces the route to a remote network host.
Connecting to Other Network Systems	
ssh	Opens secure shell connections.
telnet	Opens Telnet sessions to other hosts on the network.
Management	
copy	Copies files from one location on the device to another, from the device to a remote system, or from a remote system to the device.
restart option	Restarts the various system processes, including the routing protocol, interface, and SNMP processes.
request	Performs system-level operations, including stopping and rebooting the device and loading Junos OS images.
start	Exits the CLI and starts a UNIX shell.
configuration	Enters configuration mode.
quit	Exits the CLI and returns to the UNIX shell.

- Related Documentation**
- [MPLS Connection Checking Overview on page 1909](#)
 - [Configuring Ping MPLS on page 1911](#)
 - [Using the J-Web Ping Host Tool on page 1914](#)
 - [Using the ping Command on page 1912](#)

PART 17

Network Monitoring Using SNMP

- [SNMP Overview on page 1403](#)
- [SNMP MIBs and Traps Supported by Junos OS on page 1409](#)
- [Loading MIB Files to a Network Management System on page 1459](#)
- [Configuring SNMP on page 1463](#)
- [Configuring SNMPv3 on page 1499](#)
- [Configuring SNMP for Routing Instances on page 1541](#)
- [Configuring SNMP Remote Operations on page 1559](#)
- [Tracing SNMP Activity on page 1579](#)
- [SNMP FAQs on page 1591](#)

CHAPTER 60

SNMP Overview

- [Understanding SNMP Implementation in Junos OS on page 1403](#)
- [SNMPv3 Overview on page 1406](#)

Understanding SNMP Implementation in Junos OS

Do you use a central network management system (NMS)? Most NMS's use a version of Simple Network Management Protocol (SNMP) that can monitor the status of Junos OS devices that send unsolicited messages called traps. You can configure the IP address of your NMS so that Junos OS can send its traps.

SNMP uses a very basic form of authentication called community strings to control access between a manager and remote agents. Community strings are administrative names used to group collections of devices (and the agents running on them) into common management domains. If a manager and an agent share the same community, they can talk to one another.

Many people associate SNMP community strings with passwords and keys because the jobs they do are similar. As a result, SNMP communities are traditionally referred to as strings. The community string is the first level of management authentication implemented by the SNMP agent in Junos OS.

You might also want to configure remote logging on your device. Junos OS uses a system log (syslog) mechanism similar to many Unix devices to forward log messages to a specified log host address. This allows each of your devices to forward their messages to one central host, making it easier to monitor the network as a whole. Syslog is a very flexible and rich way of logging messages and is used by many device vendors to supplement the information provided by SNMP traps.

A typical SNMP implementation includes three components:

- Managed device
- SNMP agent
- Network management system (NMS)

A managed device is any device on a network, also known as a network element, that is managed by the network management system. Routers and switches are common examples of managed devices. The SNMP agent is the SNMP process that resides on

the managed device and communicates with the network management system. The NMS is a combination of hardware and software that is used to monitor and administer a network.

The SNMP data is stored in a highly-structured, hierarchical format known as a management information base (MIB). The MIB structure is based on a tree structure, which defines a grouping of objects into related sets. Each object in the MIB is associated with an object identifier (OID), which names the object. The “leaf” in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs in your network device.

The SNMP agent exchanges network management information with SNMP manager software running on an NMS, or host. The agent responds to requests for information and actions from the manager. The agent also controls access to the agent's MIB, the collection of objects that can be viewed or changed by the SNMP manager.

The SNMP manager collects information about network connectivity, activity, and events by polling managed devices.

Communication between the agent and the manager occurs in one of the following forms:

- **Get, GetBulk, and GetNext** requests—The manager requests information from the agent. The agent returns the information in a **Get** response message.
- **Set** requests—The manager changes the value of a MIB object controlled by the agent. The agent indicates status in a **Set** response message.
- **Traps** notification—The agent sends traps to notify the manager of significant events that occur on the network device.

The SNMP implementation in Junos OS contains:

- A master SNMP agent (known as the SNMP process or `snmpd`) that resides on the managed device and is managed by the NMS or host.
- Various subagents that reside on different modules of Junos OS, such as the Routing Engine, and are managed by the master SNMP agent (`snmpd`).



NOTE: By default, SNMP is not enabled on devices running Junos OS. For information about enabling SNMP on a device running the Junos OS, see [“Configuring SNMP on Devices Running Junos OS” on page 1471](#).

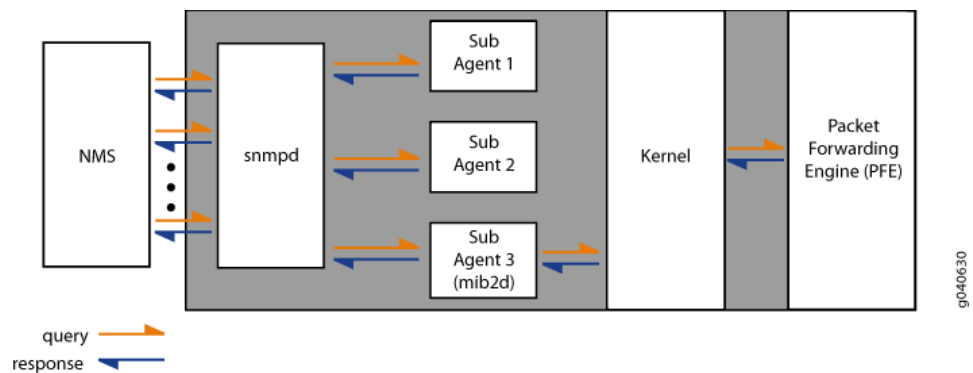
The SNMP implementation in Junos OS uses both standard (developed by the IETF and documented in RFCs) and enterprise-specific (developed and supported by specific vendors) MIBs.

In Junos OS, the management data is maintained by the `snmpd` at one level (for example, `snmpVacmMIB` and `snmpUsmMIB`), and the subagents at the next level (for example, routing MIBs and RMON MIBs). However, there is another level of data that is maintained neither by the master agent nor by the subagents. In such cases, the data is maintained

by the Junos OS processes that share the data with the subagents when polled for SNMP data. Interface-related MIBs and Firewall MIBs are good examples of data maintained by Junos OS processes.

When a network management system polls the master agent for data, the master agent immediately shares the data with the network management system if the requested data is available with the master agent or one of the subagents. However, if the requested data does not belong to those categories that are maintained by the master agent or the subagents, the subagent polls the Junos OS kernel or the process that maintains that data. On receiving the required data, the subagent passes the response back to the master agent, which in turn passes it to the NMS.

The following illustration shows the communication flow among the NMS, SNMP process (snmpd), SNMP subagents, and the Junos OS processes.



When a significant event, most often an error or a failure, occurs on a network device, the SNMP agent sends notifications to the SNMP manager. The SNMP implementation in Junos OS supports two types of notifications: traps and informs. *Traps* are unconfirmed notifications, whereas *informs* are confirmed notifications. Informs are supported only on devices that support SNMP version 3 (SNMPv3) configuration.

Junos OS supports trap queuing to ensure that traps are not lost because of temporary unavailability of routes. Two types of queues, *destination queues* and a *throttle queue*, are formed to ensure delivery of traps and to control the trap traffic.

Junos OS forms a destination queue when a trap to a particular destination is returned because the host is not reachable, and adds the subsequent traps to the same destination to the queue. Junos OS checks for availability of routes every 30 seconds and sends the traps from the destination queue in a round-robin fashion.

If the trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts occur at progressive intervals of 1 minute, 2 minutes, 4 minutes, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is 10. After 10 unsuccessful attempts, the destination queue and all the traps in the queue are deleted.

Junos OS also has a throttle mechanism to control the number of traps (throttle threshold; default value of 500 traps) sent during a particular time period (throttle interval; default

of 5 seconds) and to ensure consistency in trap traffic, especially when large number of traps are generated because of interface status changes. The throttle interval period begins when the first trap arrives at the throttle. All traps within the trap threshold are processed, and the traps beyond the threshold limit are queued.

The maximum size of trap queues—that is, throttle queue and destination queue put together—is 40,000. However, on EX Series Ethernet Switches, the maximum size of the trap queue is 1,000. The maximum size of any one queue is 20,000 for devices other than EX Series Switches. On EX Series Switches, the maximum size of one queue is 500. When a trap is added to the throttle queue, or if the throttle queue has exceeded the maximum size, the trap is added back on top of the destination queue, and all subsequent attempts from the destination queue are stopped for a 30-second period, after which the destination queue restarts sending the traps.

Related Documentation

- [FAQ: SNMP Support on Junos OS](#)
- [Configuring SNMP on Devices Running Junos OS on page 1471](#)
- [Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS on page 1579](#)
- [Optimizing the Network Management System Configuration for the Best Results on page 1467](#)
- [Configuring Options on Managed Devices for Better SNMP Response Time on page 1469](#)
- *Managing Traps and Informs*
- *Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage*

SNMPv3 Overview

In contrast to SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2), SNMP version 3 (SNMPv3) supports authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.

USM uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured for both the agent and the manager. Messages sent using USM are better protected than messages sent with community strings, where passwords are sent in the clear. With USM, messages exchanged between the manager and the agent can have data integrity checking and data origin authentication. USM protects against message delays and message replays by using time indicators and request IDs. Encryption is also available.

To complement the USM, SNMPv3 uses the VACM, a highly granular access-control model for SNMPv3 applications. Based on the concept of applying security policies to the name of the groups querying the agent, the agent decides whether the group is allowed to view or change specific MIB objects. VACM defines collections of data (called views), groups of data users, and access statements that define which views a particular group of users can use for reading, writing, or receiving traps.

Trap entries in SNMPv3 are created by configuring the notify, notify filter, target address, and target parameters. The **notify** statement specifies the type of notification (trap) and contains a single tag. The tag defines a set of target addresses to receive a trap. The notify filter defines access to a collection of trap object identifiers (OIDs). The target address defines a management application's address and other attributes to be used in sending notifications. Target parameters define the message processing and security parameters to be used in sending notifications to a particular management target.

To configure SNMPv3, perform the following tasks:

- [Creating SNMPv3 Users on page 1507](#)
- [Configuring MIB Views on page 1496](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring SNMP Informs on page 1529](#)

**Related
Documentation**

- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

SNMP MIBs and Traps Supported by Junos OS

- Standard SNMP MIBs Supported by Junos OS on page 1409
- Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427
- Enterprise-Specific MIBs and Supported Devices on page 1439
- SNMP MIB Objects Supported by Junos OS for the SNMP Set Operation on page 1449
- Standard SNMP Traps Supported on Devices Running Junos OS on page 1456
- Juniper Networks Enterprise-Specific SNMP Traps on page 1456

Standard SNMP MIBs Supported by Junos OS

Table 111 contains the list of standard SNMP MIBs and RFCs that are supported on various devices running Junos OS. RFCs can be found at <http://www.ietf.org>.



NOTE: In this table, a value of 1 in any of the platform columns (ACX, M, T, MX, EX, PTX, and SRX) denotes that the corresponding MIB is supported on that particular platform, and a value of 0 denotes that the MIB is not supported on the platform.

Table 111: Standard MIBs Supported on Devices Running Junos OS

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
IEEE 802.1ab section 12.1, <i>Link Layer Discovery Protocol (LLDP) MIB</i>	0	0	0	1	1	0	0	0	0
EX Series implementation of LLDP MIB supports both IPv4 and IPv6 configuration.									
For more information about LLDP MIB objects supported on EX Series devices, see <i>LLDP Standard MIB Objects Supported on EX Series Devices</i> .									
IEEE, 802.3ad, <i>Aggregation of Multiple Link Segments</i>	0	1	1	1	1	1	1	1	1
Supported tables and objects:									
<ul style="list-style-type: none"> dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable 									
NOTE: EX Series switches do not support the dot3adAggPortTable and dot3adAggPortStatsTable .									
<ul style="list-style-type: none"> dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount) 									
NOTE: EX Series switches do not support the dot3adAggPortDebugTable .									
<ul style="list-style-type: none"> dot3adTablesLastChanged 									

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
IEEE, 802.1ag, <i>Connectivity Fault Management</i>	0	0	0	1	0	0	0	0	

Supported tables and objects:

- dot1agCfmMdTableNextIndex
- dot1agCfmMdTable (except dot1agCfmMdMhfdPermission)
- dot1agCfmMaNetTable
- dot1agCfmMaMepListTable
- dot1agCfmDefaultMdDefLevel
- dot1agCfmDefaultMdDefMhfCreation
- dot1agCfmMepTable (except dot1agCfmMepLbrBadMsdu, dot1agCfmMepTransmitLbmVlanPriority, dot1agCfmMepTransmitLbmVlanDropEnable, dot1agCfmMepTransmitLtmFlags, dot1agCfmMepPbbTeCanReportPbbTePresence, dot1agCfmMepPbbTeTrafficMismatchDefect, dot1agCfmMepPbbTransmitLbmLtmReverseVid, dot1agCfmMepPbbTeMismatchAlarm, dot1agCfmMepPbbTeLocalMismatchDefect, and dot1agCfmMepPbbTeMismatchSinceReset)
- dot1agCfmLtrTable (except dot1agCfmLtrChassisIdSubtype, dot1agCfmLtrChassisId, dot1agCfmLtrManAddressDomain, dot1agCfmLtrManAddress, dot1agCfmLtrIngressPortIdSubtype, dot1agCfmLtrIngressPortId, dot1agCfmLtrEgressPortIdSubtype, dot1agCfmLtrEgressPortId, and dot1agCfmLtrOrganizationSpecificTlv)
- dot1agCfmMepDbTable (except dot1agCfmMebDbChassisIdSubtype, dot1agCfmMebDbChassisId, dot1agCfmMebDbManAddressDomain, and dot1agCfmMebDbManAddress)

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
IEEE, 802.1ap, <i>Management Information Base (MIB) definitions for VLAN Bridges</i>	0	0	0	1	0	0	0	0	
Supported tables and objects:									
<ul style="list-style-type: none"> • <code>ieee8021CfmStackTable</code> • <code>ieee8021CfmVlanTable</code> • <code>ieee8021CfmDefaultMdTable</code> (except <code>ieee8021CfmDefaultMdIdPermission</code>) • <code>ieee8021CfmMaCompTable</code> (except <code>ieee8021CfmMaCompldPermission</code>) 									
RFC 1155, <i>Structure and Identification of Management Information for TCP/IP-based Internets</i>	1	1	1	1	1	1	1	1	1
RFC 1157, <i>A Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	1	1	1
RFC 1195, <i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i> (only the objects <code>isisSystem</code> , <code>isisMANAreaAddr</code> , <code>isisAreaAddr</code> , <code>isisSysProtSupp</code> , <code>isisSummAddr</code> , <code>isisCirc</code> , <code>isisCircLevel</code> , <code>isisPacketCount</code> , <code>isisSAdj</code> , <code>isisSAdjAreaAddr</code> , <code>isisAdjIPAddr</code> , <code>isisSAdjProtSupp</code> , <code>isisRa</code> , and <code>isisIPRA</code> are supported)	1	1	1	1	1	1	1	1	1
RFC 1212, <i>Concise MIB Definitions</i>	1	1	1	1	1	1	0	0	1
RFC 1213, <i>Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II</i> . Junos OS supports the following areas:	1	1	1	1	1	1	0	0	1
<ul style="list-style-type: none"> • MIB II and its SNMP version 2 derivatives, including: <ul style="list-style-type: none"> • Statistics counters • IP, except for <code>ipRouteTable</code>, which has been replaced by <code>ipCidrRouteTable</code> (RFC 2096, <i>IP Forwarding Table MIB</i>) • SNMP management • Interface management • SNMPv1 <code>Get</code>, <code>GetNext</code> requests, and version 2 <code>GetBulk</code> request • Junos OS-specific secured access list • Master configuration keywords • Reconfigurations upon SIGHUP 									

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 1215, <i>A Convention for Defining Traps for use with the SNMP</i> (only MIB II SNMP version 1 traps and version 2 notifications)	1	1	1	1	1	1	0	0	1
RFC 1406, <i>Definitions of Managed Objects for the DS1 and E1 Interface Types</i> (T1 MIB is supported)	1	1	1	0	0	0	1	0	0
RFC 1407, <i>Definitions of Managed Objects for the DS3/E3 Interface Type</i> (T3 MIB is supported)	0	1	1	0	0	0	0	0	0
RFC 1471, <i>Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol</i> (only pppLink group is supported. The pppLink group consists of the pppLcp 1 object and the tables pppLinkStatustable and pppLinkConfigTable).	0	1	0	1	0	1	0	0	0
RFC 1657, <i>Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2</i>	1	1	1	1	1	0	0	0	0
RFC 1695, <i>Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2</i>	1	1	1	0	0	1	0	0	0
RFC 1850, <i>OSPF Version 2 Management Information Base</i> (except for the ospfOriginateNewLsas and ospfRxNewLsas objects, the Host Table, and the traps ospfOriginateLSA , ospfLsdbOverflow , and ospfLsdbApproachingOverflow)	1	1	1	1	1	1	1	0	0
RFC 1901, <i>Introduction to Community-based SNMPv2</i>	1	1	1	1	1	1	1	1	1
RFC 2011, <i>SNMPv2 Management Information Base for the Internet Protocol Using SMIv2</i>	1	1	1	1	1	1	0	0	0
RFC 2012, <i>SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2</i>	1	1	1	1	1	1	1	0	1
RFC 2013, <i>SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2</i>	1	1	1	1	1	1	1	0	1

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 2024, <i>Definitions of Managed Objects for Data Link Switching Using SMIv2</i> (except for the dlswInterface and dlswSdlc object groups; the dlswDirLocateMacTable , dlswDirNBTable , and dlswDirLocateNBTable tables; the dlswCircuitDiscReasonLocal and dlswCircuitDiscReasonRemote tabular objects; and the dlswDirMacCacheNextIndex and dlswDirNBCacheNextIndex scalar objects; read-only access)	0	1	1	1	0	0	0	0	0
RFC 2096, <i>IP Forwarding Table MIB</i> (The ipCidrRouteTable has been extended to include the tunnel name when the next hop is through an RSVP-signaled LSP.) NOTE: RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.	1	1	1	1	1	1	0	0	1
RFC 2115, <i>Management Information Base for Frame Relay DTEs Using SMIv2</i> (frDlcmiTable only; frCircuitTable and frErrTable are not supported)	0	1	1	1	0	0	1	0	0
RFC 2233, <i>The Interfaces Group MIB Using SMIv2</i> NOTE: RFC 2233 has been replaced by RFC 2863, IF MIB. However, Junos OS supports both RFC 2233 and RFC 2863.	1	1	1	1	1	1	1	0	1
RFC 2287, <i>Definitions of System-Level Managed Objects for Applications</i> (only the objects sysApplInstallIPkgTable , sysApplInstallElmtTable , sysApplElmtRunTable , and sysApplMapTable)	1	1	1	1	1	1	1	0	1
RFC 2465, <i>Management Information Base for IP Version 6: Textual Conventions and General Group</i> (except for IPv6 interface statistics)	1	1	1	1	0	1	1	0	0
RFC 2495, <i>Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types</i> (except for dsx1FarEndConfigTable , dsx1FarEndCurrentTable , dsx1FarEndIntervalTable , dsx1FarEndTotalTable , and dsx1FracTable)	1	1	1	0	0	0	1	0	0
RFC 2515, <i>Definitions of Managed Objects for ATM Management</i> (except atmVpCrossConnectTable , atmVcCrossConnectTable , and aal5VccTable)	1	1	1	0	0	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 2570, <i>Introduction to Version 3 of the Internet-standard Network Management Framework</i>	1	1	1	1	1	1	0	0	1
RFC 2571, <i>An Architecture for Describing SNMP Management Frameworks</i> (read-only access)	1	1	1	1	1	1	1	0	1
NOTE: RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.									
RFC 2572, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i> (read-only access)	1	1	1	1	1	1	1	0	1
NOTE: RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.									
RFC 2576, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	1	1	1	1	1	1	1	0	1
NOTE: RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.									
RFC 2578, <i>Structure of Management Information Version 2 (SMIv2)</i>	1	1	1	1	1	1	0	0	1
RFC 2579, <i>Textual Conventions for SMIv2</i>	1	1	1	1	1	1	0	0	1
RFC 2580, <i>Conformance Statements for SMIv2</i>	1	1	1	1	1	1	0	0	1
RFC 2662, <i>Definitions of Managed Objects for ADSL Lines</i>	0	1	1	1	0	0	1	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 2665, <i>Definitions of Managed Objects for the Ethernet-like Interface Types</i>	1	1	1	1	1	1	1	0	1
<p>NOTE: For M, T and MX Series, the SNMP counters do not count the Ethernet header and frame check sequence (FCS). Therefore, the Ethernet header bytes and the FCS bytes are not included in the following four OIDs:</p> <ul style="list-style-type: none"> • ifInOctets • ifOutOctets • ifHCInOctets • ifHCOctets <p>However, the EX switches adhere to RFC 2665.</p> <p>NOTE: The list of managed objects specified in RFC 2665 has been updated by RFC 3635 by including information useful for the management of 10 Gigabit per second Ethernet interfaces.</p>									
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol (except row creation, the Set operation, and the object vrrpStatsPacketLengthErrors)</i>	1	1	1	1	1	1	1	0	1
RFC 2790, <i>Host Resources MIB</i>	1	1	1	1	1	1	1	0	1
<ul style="list-style-type: none"> • Only the hrStorageTable. The file systems /, /config, /var, and /tmp always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change. • Only the objects of the hrSystem and hrSWInstalled groups. 									
RFC 2819, <i>Remote Network Monitoring Management Information Base</i>	1	1	1	1	1	1	1	0	1
<ul style="list-style-type: none"> • etherStatsTable (for Ethernet interfaces only), alarmTable, eventTable, and logTable are supported on all devices running Junos OS. • historyControlTable and etherHistoryTable (except etherHistoryUtilization object) are supported only on EX Series switches. 									

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 2863, <i>The Interfaces Group MIB</i>	1	1	1	1	1	1	0	0	1
NOTE: RFC 2863 replaces RFC 2233. However, Junos OS supports both RFC 2233 and RFC 2863.									
RFC 2864, <i>The Inverted Stack Table Extension to the Interfaces Group MIB</i>	0	1	1	1	0	1	0	0	1
RFC 2922, <i>The Physical Topology (PTOPO) MIB</i>	0	0	0	0	1	0	1	0	1
Supported objects: ptopoConnDiscAlgorithm, ptopoConnAgentNetAddrType, ptopoConnAgentNetAddr, ptopoConnMultiMacSASeen, ptopoConnMultiNetSASeen, ptopoConnsStatic, ptopoConnLastVerifyTime, ptopoConnRowStatus									
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i> (only the objects pingCtlTable , pingResultsTable , pingProbeHistoryTable , pingMaxConcurrentRequests , traceRouteCtlTable , traceRouteResultsTable , traceRouteProbeHistoryTable , and traceRouteHopsTable)	1	1	1	1	1	1	1	0	1
RFC 2932, <i>IPv4 Multicast Routing MIB</i>	1	1	1	1	1	1	1	0	1
RFC 2934, <i>Protocol Independent Multicast MIB for IPv4</i>	1	1	1	1	1	1	1	0	0
NOTE: In Junos OS, RFC 2934 is implemented based on a draft version, <i>pimmib.mib</i> , of the now standard RFC. Support for the pimNeighborLoss trap was added in Release 11.4.									
RFC 2981, <i>Event MIB</i>	1	1	1	1	0	1	0	0	0
RFC 3014, <i>Notification Log MIB</i>	1	1	1	1	0	1	0	0	0
RFC 3019, <i>IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol</i>	0	1	1	1	0	1	0	0	1

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 3410 <i>Introduction and Applicability Statements for Internet-Standard Management Framework</i>	1	1	1	1	1	1	0	0	1
RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i>	1	1	1	1	1	1	0	0	1
NOTE: RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.									
RFC 3412, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	0	0	1
NOTE: RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.									
RFC 3413, <i>Simple Network Management Protocol (SNMP) Applications</i> (except for the Proxy MIB)	1	1	1	1	1	1	1	0	1
RFC 3414, <i>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</i>	1	1	1	1	1	1	0	0	1
RFC 3415, <i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	0	0	1
RFC 3416, <i>Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	0	0	1
NOTE: RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.									
RFC 3417, <i>Transport Mappings for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	1	0	1
RFC 3418, <i>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	1	0	0	1
NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.									
RFC 3498, <i>Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures</i> (implemented under the Juniper Networks enterprise branch [jnxExperiment])	0	1	1	0	0	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 3584 <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	1	1	1	1	1	1	0	0	1
RFC 3591 <i>Managed Objects for the Optical Interface Type</i>	0	1	1	0	0	0	0	0	0
optIfOTMnTable (except optIfOTMnOpticalReach , optIfOTMnInterfaceType , and optIfOTMnOrder), optIfOChConfigTable (except optIfOChDirectionality and optIfOChCurrentStatus), optIfOTUkConfigTable (except optIfOTUkTraceIdentifierAccepted , optIfOTUkTIMDetMode , optIfOTUkTIMActEnabled , optIfOTUkTraceIdentifierTransmitted , optIfOTUkDEGThr , optIfOTUkDEGM , optIfOTUkSinkAdaptActive , and optIfOTUkSourceAdaptActive), and optIfODUkConfigTable (except optIfODUkPositionSeqCurrentSize and optIfODUkTtpPresent)									
RFC 3592, <i>Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type</i>	0	1	1	1	0	0	0	0	0
RFC 3621, <i>Power Ethernet MIB</i>	0	0	0	0	1	0	0	0	0
RFC 3635, <i>Definitions of Managed Objects for the Ethernet-like Interface Types</i> (except dot3StatsRateControlAbility and dot3StatsRateControlStatus in dot3StatsEntry table)	0	0	0	1	0	0	0	0	0
NOTE: The values of the following objects in dot3HCStatsEntry table will be always zero for both 32-bit counters and 64-bit counters: <ul style="list-style-type: none"> dot3HCStatsSymbolErrors dotHCStatsInternalMacTransmitErrors 									
RFC 3637, <i>Definitions of Managed Objects for the Ethernet WAN Interface Sublayer</i> (except etherWisDeviceTable , etherWisSectionCurrentTable , and etherWisFarEndPathCurrentTable)	0	1	1	1	0	1	0	0	0
RFC 3811, <i>Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management</i>	1	1	1	1	0	1	1	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 3812, <i>Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)</i> (read only access)	1	1	1	1	0	1	0	0	0
<ul style="list-style-type: none"> MPLS tunnels as interfaces are not supported. The following objects in the TunnelResource table are not supported: <code>mplsTunnelResourceMeanRate</code>, <code>mplsTunnelResourceMaxBurstSize</code>, <code>mplsTunnelResourceMeanBurstSize</code>, <code>mplsTunnelResourceExBurstSize</code>, <code>mplsTunnelResourceWeight</code>. <code>mplsTunnelPerfTable</code> and <code>mplsTunnelCRLDPResTable</code> are not supported. <code>mplsTunnelCHopTable</code> is supported on ingress routers only. <p>NOTE: The branch used by the proprietary LDP MIB (<code>ldpmib.mib</code>) conflicts with RFC 3812. <code>ldpmib.mib</code> has been deprecated and replaced by <code>jnx-mpls-ldp.mib</code>.</p>									
RFC 3813, <i>Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)</i> (read-only access). <code>mplsInterfacePerfTable</code> , <code>mplsInSegmentPerfTable</code> , <code>mplsOutSegmentPerfTable</code> , <code>mplsInSegmentMapTable</code> , <code>mplsXCUp</code> , and <code>mplsXCDown</code> are not supported.	1	1	1	1	0	1	1	0	0
RFC 3826, <i>The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model</i>	1	1	1	1	1	1	0	0	1
RFC 3877, <i>Alarm Management Information Base</i> except:	0	0	0	1	0	0	0	0	
<ul style="list-style-type: none"> Junos OS does not support the alarmActiveStatsTable. Traps that do not conform to the alarm model are not supported. However, these traps can be redefined to conform to the alarm model. 									
RFC 3896, <i>Definitions of Managed Objects for the DS3/E3 Interface Type</i> (except <code>dsx3FarEndConfigTable</code> , <code>dsx3FarEndCurrentTable</code> , <code>dsx3FarEndIntervalTable</code> , <code>dsx3FarEndTotalTable</code> , and <code>dsx3FracTable</code>)	0	1	1	0	0	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 4087, <i>IP Tunnel MIB</i> —Describes MIB objects in the following tables for managing tunnels of any type over IPv4 and IPv6 networks: <ul style="list-style-type: none"> • tunnelIfTable—Provides information about the tunnels known to a router. • tunnelInetConfigTable—Assists dynamic creation of tunnels and provides mapping from end-point addresses to the current interface index value. NOTE: Junos OS supports MAX-ACCESS of read-only for all the MIB objects in tunnelIfTable and tunnelInetConfigTable tables.	0	1	1	1	0	0	0	0	0
RFC 4133, <i>Entity MIB</i> —Supports tables and objects except: <ul style="list-style-type: none"> • entityLogicalGroup table • entPhysicalMfgDate and entPhysicalUris objects in entityPhysical2Group table • entLPMappingTable and entPhysicalContainsTable in entityMappingGroup table • entityNotificationsGroup table NOTE: Supported only on MX240, MX480, and MX960 routers, and EX2200 and EX3300 switches.	0	0	0	1	1	0	0	0	
RFC 4188, <i>Definitions of Managed Objects for Bridges</i> —Supports 802.1D STP (1998). Supports only the following subtrees and objects: <ul style="list-style-type: none"> • dot1dStp subtree is supported on MX Series 3D Universal Edge Routers. • dot1dTpFdbAddress, dot1dTpFdbPort, and dot1dTpFdbStatus objects from the dot1dTpFdbTable of the dot1dTp subtree are supported on EX Series Ethernet Switches. NOTE: dot1dTpLearnedEntryDiscards and dot1dTpAgingTime objects are supported on M and T Series routers.	0	0	0	1	1	0	0	0	
RFC 4268, <i>Entity State MIB</i> —Junos OS supports all objects and tables. NOTE: Supported only on MX240, MX480, and MX960 routers, and EX2200 and EX3300 switches.	0	0	0	1	1	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 4273, <i>Definitions of Managed Objects for BGP-4</i> (only <code>jnxBgpM2PrefixInPrefixes</code> , <code>jnxBgpM2PrefixInPrefixesAccepted</code> , and <code>jnxBgpM2PrefixInPrefixesRejected</code> objects)	1	1	1	1	1	0	0	0	1
RFC 4292, <i>IP Forwarding MIB</i> — Describes a table and MIB objects for forwarding IP packets that are version independent: <ul style="list-style-type: none"> <code>inetCidrRouteTable</code>—Provides the ability to display IP version-independent multipath CIDR routes and obsoletes the <code>ipCidrRouteTable</code> object. <code>inetCidrRouteNumber</code>—Indicates the number of current routes and obsoletes the <code>ipCidrRouteNumber</code> object. <code>inetCidrRouteDiscards</code>—Counts the number of valid routes that are discarded from <code>inetCidrRouteTable</code> and obsoletes the <code>ipCidrRouteDiscards</code> object. <p>NOTE: Junos OS currently supports these MIB objects that will be deprecated in future releases: <code>ipCidrRouteTable</code>, <code>ipCidrRouteNumber</code>, and <code>ipCidrRouteDiscards</code>.</p>	1	1	1	1	1	1	0	0	0
RFC 4293, <i>Management Information Base for the Internet Protocol (IP)</i> — Supports only the mandatory groups. For detailed information, see Standard IPv4/IPv6 MIBs .	0	0	0	1	1	0	0	0	0
RFC 4318, <i>Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol</i> —Supports 802.1w and 802.1t extensions for RSTP.	0	1	1	1	1	0	0	0	0
RFC 4363b, <i>Q-Bridge VLAN MIB</i>	0	0	0	1	1	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 4382 <i>MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB</i>	0	1	1	1	1	1	0	0	0
<p>The Junos OS support for RFC 4382 includes the following scalar objects and tables:</p> <ul style="list-style-type: none"> • <code>mplsL3VpnActiveVrfs</code> • <code>mplsL3VpnConfiguredVrfs</code> • <code>mplsL3VpnConnectedInterfaces</code> • <code>mplsL3VpnVrfConfMidRteThresh</code> • <code>mplsL3VpnVrfConfHighRteThresh</code> • <code>mplsL3VpnIfConfRowStatus</code> • <code>mplsL3VpnIfLblRcvThrsh</code> • <code>mplsL3VpnNotificationEnable</code> • <code>mplsL3VpnVrfConfMaxPossRts</code> • <code>mplsL3VpnVrfConfRteMxThrshTime</code> • <code>mplsL3VpnVrfOperStatus</code> • <code>mplsL3VpnVrfPerfCurrNumRoutes</code> • <code>mplsL3VpnVrfPerfTable</code> • <code>mplsL3VpnVrfRteTable</code> • <code>mplsVpnVrfRTTable</code> • <code>mplsL3VpnVrfTable</code> <p>NOTE: The <code>mplsL3VpnIfConfTable</code> has not been implemented in the MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB, because of limited utility and difficulty in representing the <code>DistProtocol</code> bit accurately.</p>									
RFC 4444, <i>IS-IS MIB</i>	1	1	1	1	1	1	1	0	0
RFC 4668, <i>RADIUS Accounting Client Management Information Base (MIB) for IPv6</i> (read-only access)	0	0	0	1	0	0	0	0	0
RFC 4670, <i>RADIUS Accounting Client Management Information Base (MIB)</i> (read-only access)	0	0	0	1	0	0	0	0	0
RFC 4801, <i>Definitions of Textual Conventions for Generalized Multiprotocol Label Switching (GMPLS) Management Information Base (MIB)</i> (read-only access)	0	1	1	1	0	0	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 4802, <i>Generalized Multiprotocol Label Switching (GMPLS) Traffic Engineering (TE) Management Information Base (MIB)</i> (read-only access). gmplsTunnelReversePerfTable , gmplsTeScalars , gmplsTunnelTable , gmplsTunnelARHopTable , gmplsTunnelCHopTable , and gmplsTunnelErrorTable are not supported.)	0	1	1	1	0	0	0	0	0
RFC 4803, <i>Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base (MIB)</i> (read-only access). gmplsLabelTable and gmplsOutsegmentTable are not supported.	0	1	1	1	0	0	0	0	0
NOTE: The tables in GMPLS TE (RFC 4802) and LSR (RFC 4803) MIBs are extensions of the corresponding tables from the MPLS TE (RFC 3812) and LSR (RFC 3813) MIBs and use the same index as the MPLS MIB tables.									

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RFC 5643, <i>Management Information Base for OSPFv3</i>	0	1	1	1	0	1	0	0	1
<p>NOTE: Junos OS support for this MIB is read-only.</p> <p>Junos OS does not support the following tables and objects defined in this MIB.</p> <ul style="list-style-type: none"> • ospfv3HostTable • ospfv3CfgNbrTable • ospfv3ExitOverflowInterval • ospfv3ReferenceBandwidth • ospfv3RestartSupport • ospfv3RestartInterval • ospfv3RestartStrictLsaChecking • ospfv3RestartStatus • ospfv3RestartAge • ospfv3RestartExitReason • ospfv3NotificationEnable • ospfv3StubRouterSupport • ospfv3StubRouterAdvertisement • ospfv3DiscontinuityTime • ospfv3RestartTime • ospfv3AreaNssaTranslatorRole • ospfv3AreaNssaTranslatorState • ospfv3AreaNssaTranslatorStabInterval • ospfv3AreaNssaTranslatorEvents • ospfv3AreaTEEnabled • ospfv3IfMetricValue • ospfv3IfDemandNbrProbe 									
RFC 6527, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)</i> (except row creation, the Set operation, and the objects vrrpv3StatisticsRowDiscontinuityTime and vrrpv3StatisticsPacketLengthErrors)	1	0	0	0	0	0	0	0	0
Internet Assigned Numbers Authority, <i>IANAiftype Textual Convention MIB</i> (referenced by RFC 2233, available at http://www.iana.org/assignments/ianaiftype-mib)	1	1	1	1	1	1	1	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Internet draft draft-ietf-atommib-sonetaps-mib-10.txt, <i>Definitions of Managed Objects for SONET Linear APS Architectures</i> (as defined under the Juniper Networks enterprise branch [jnxExperiment] only)	0	1	1	1	0	0	0	0	0
Internet draft draft-ietf-bfd-mib-02.txt, <i>Bidirectional Forwarding Detection Management Information Base</i> (Represented by mib-jnx-bfd-exp.txt and implemented under the Juniper Networks enterprise branch [jnxExperiment]. Read only. Includes bfdSessUp and bfdSessDown traps. Does not support bfdSessPerfTable and bfdSessMapTable .)	1	1	1	1	1	0	0	0	1
Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, <i>MPLS/BGP Layer 3 VPN Multicast Management Information Base</i> (Implemented under the Juniper Networks enterprise branch [jnxExperiment]. OID for jnxMvpnExperiment is .1.3.6.1.4.1.2636.5.12. Read only. Includes jnxMvpnNotifications traps.)	0	1	1	0	0	0	0	0	
Internet draft draft-ietf-idmr-igmp-mib-13.txt, <i>Internet Group Management Protocol (IGMP) MIB</i>	0	1	1	1	1	1	0	0	1
Internet draft draft-reeder-snmppv3-usm-3desede-00.txt, <i>Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode</i>	1	1	1	1	1	1	0	0	1
Internet draft draft-ietf-isis-wg-mib-07.txt, <i>Management Information Base for IS-IS</i> (only isisSAdjTable , isisSAdjAreaAddrTable , isisSAdjIPAddrTable , and isisSAdjProtSuppTable) NOTE: Replaced with RFC 4444, <i>IS-IS MIB</i> in Junos OS Release 11.3 and later.	1	1	1	1	1	1	1	0	0
Internet draft draft-ietf-ppvpn-mpls-vpn-mib-04.txt, <i>MPLS/BGP Virtual Private Network Management Information Base Using SMIv2</i> (only mplsVpnScalars , mplsVpnVrfTable , mplsVpnPerTable , and mplsVpnVrfRouteTargetTable)	0	1	1	1	0	1	0	0	0

Table 111: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, <i>Management Information Base for OSPFv3</i> (Represented by <code>mib-jnx-ospfv3mib.txt</code> and implemented under the Juniper Networks enterprise branch <code>{jnxExperiment}</code> . Support for <code>ospfv3NbrTable</code> only. Read only. Object names are prefixed by <code>jnx</code> . For example, <code>jnxOspfv3NbrTable</code> , <code>jnxOspfv3NbrAddressType</code> , and <code>jnxOspfv3NbrPriority</code> .)	0	1	1	1	0	1	0	0	1
Internet draft draft-ietf-idmr-pim-mib-09.txt, <i>Protocol Independent Multicast (PIM) MIB</i>	1	1	1	1	1	1	0	0	1
ESO Consortium MIB, which can be found at http://www.snmp.com/eso/ NOTE: The ESO Consortium MIB has been replaced by RFC 3826.	1	1	1	1	1	1	1	0	0
Internet Draft P2MP MPLS-TE MIB (draft-ietf-mpls-p2mp-te-mib-09.txt) (read-only access) (except <code>mplsTeP2mpTunnelBranchPerfTable</code>).	1	1	1	1	0	1	0	0	0

- Related Documentation**
- [Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427](#)
 - [Loading MIB Files to a Network Management System on page 1459](#)

Enterprise-Specific SNMP MIBs Supported by Junos OS

Junos OS supports the following enterprise-specific MIBs:

- **AAA Objects MIB**—Provides support for monitoring user authentication, authorization, and accounting through the RADIUS, LDAP, SecurID, and local authentication servers. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-user-aaa.txt. For more information, see *AAA Objects MIB*.
- **Access Authentication Objects MIB**—Provides support for monitoring firewall authentication, including data about the users trying to access firewall-protected resources and the firewall authentication service itself. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-auth.txt.

For more information, see *Access Authentication Objects MIB*.

- Alarm MIB—Provides support for alarms from the router. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chassis-alarm.txt

For more information, see *Alarm MIB*.

- Analyzer MIB—Contains analyzer and remote analyzer data related to port mirroring on the EX Series Ethernet Switches. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-analyzer.txt

For more information, see *Analyzer MIB*.

- Antivirus Objects MIB—Provides information about the antivirus engine, antivirus scans, and antivirus scan-related traps. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-utm-av.txt

For more information, see *Antivirus Objects MIB*.

- ATM Class-of-Service MIB—Provides support for monitoring Asynchronous Transfer Mode, version 2 (ATM2) virtual circuit (VC) class-of-service (CoS) configurations. It also provides CoS queue statistics for all VCs that have CoS configured. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-atm-cos.txt

For more information, see *ATM Class-of-Service MIB*.

- ATM MIB—Provides support for ATM interfaces and virtual connections. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-atm.txt.

For more information, see *ATM MIB*.

- BGP4 V2 MIB—Contains objects used to monitor BGP peer-received prefix counters. It is based upon similar objects in the MIB documented in Internet draft draft-ietf-idr-bgp4-mibv2-03.txt, *Definitions of Managed Objects for the Fourth Version of BGP (BGP-4), Second Version*. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-bgpmib2.txt

For more information, see *BGP4 V2 MIB*.

- Bidirectional Forwarding Detection MIB—Provides support for monitoring Bidirectional Forwarding Detection (BFD) sessions. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-bfd.txt

For more information, see *Bidirectional Forwarding Detection MIB*.

- Chassis Definitions for Router Model MIB—Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify platform and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chas-defines.txt

For more information, see *Chassis MIBs*.

- Chassis MIB—Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and air flow) and inventory support for the chassis, System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), Flexible PIC Concentrators (FPCs), and PICs. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chassis.txt

For more information, see *Chassis MIBs*.

- Chassis Cluster MIB—Provides information about objects that are used whenever the state of the control link interfaces or fabric link interfaces changes (up to down or down to up) in a chassis cluster deployment. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jsrpd.txt

For more information, see *Chassis Cluster MIB*.

- Class-of-Service MIB—Provides support for monitoring interface output queue statistics per interface and per forwarding class. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-cos.txt

For more information, see *Class-of-Service MIB*.

- Configuration Management MIB—Provides notification for configuration changes as SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in `jnxCmChgEventTable`. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-cfgmgmt.txt

For more information, see *Configuration Management MIB*.

- Destination Class Usage MIB—Provides support for monitoring packet counts based on the ingress and egress points for traffic transiting your networks. Ingress points are identified by the input interface. Egress points are identified by destination prefixes grouped into one or more sets, known as destination classes. One counter is managed per interface per destination class, up to a maximum of 16 counters per interface. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dcu.txt

For more information, see *Destination Class Usage MIB*.

- DHCP Objects MIB— Provides SNMP support (get and trap) for DHCP local server and relay configurations. It also provides support for bindings and leases tables, and for statistics. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jdhcp.txt

For more information, see *DHCP MIB*.

- DHCPv6 MIB—Provides SNMP support (get and trap) for DHCPv6 local server and relay configurations. It also provides support for bindings and leases tables, and for statistics. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jdhcpv6.txt

For more information, see *DHCPv6 MIB*.

- Digital Optical Monitoring MIB—Provides support for the **SNMP Get** request for statistics and **SNMP Trap** notifications for alarms. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dom.txt
For more information, see *Digital Optical Monitoring MIB*.
- DNS Objects MIB—Provides support for monitoring DNS proxy queries, requests, responses, and failures. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-dns.txt
For more information, see *DNS Objects MIB*.
- Dynamic Flow Capture MIB—Provides support for monitoring the operational status of dynamic flow capture (DFC) PICs. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dfc.txt
For more information, see *Dynamic Flow Capture MIB*.
- Ethernet MAC MIB—Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, **inoctets**, **inframes**, **outoctets**, and **outframes** on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mac.txt
For more information, see *Ethernet MAC MIB*.
- Event MIB—Defines a generic trap that can be generated using an op script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-event.txt
For more information, see *Event MIB*.
- Experimental MIB—Contains object identifiers for experimental MIBs. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-exp.txt
For more information, see *jnxExperiment MIB*.
- Firewall MIB—Provides support for monitoring firewall filter counters. Routers must have the Internet Processor II ASIC to perform firewall monitoring. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-firewall.txt
For more information, see *Firewall MIB*.
- Flow Collection Services MIB—Provides statistics on files, records, memory, FTP, and error states of a monitoring services interface. It also provides SNMP traps for unavailable destinations, unsuccessful file transfers, flow overloading, and memory overloading. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-coll.txt
For more information, see *Flow Collection Services MIB*.
- Host Resources MIB—Extends the **hrStorageTable** object, providing a measure of the usage of each file system on the router in percentage format. Previously, the objects

in the **hrStorageTable** measured the usage in allocation units—**hrStorageUsed** and **hrStorageAllocationUnits**—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-hostresources.txt

For more information, see *Host Resources MIB*.

- IDP Objects MIB—Provides support for monitoring SNMP IDP queries, requests, responses, and failures. This MIB defines the key monitoring and threshold crossing trap support, IDP database update status and trap support, attack-related monitoring and trap support for SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways. This MIB models IDP attributes specific to the appropriate Juniper Networks implementation. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-idp.txt

For more information, see *IDP MIB*.

- Interface MIB—Extends the standard **ifTable** (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-if-extensions.txt

For more information, see *Interface MIB*.

- Interface Accounting Forwarding Class MIB—Extends the Juniper Enterprise Interface MIB and provides support for monitoring statistics data for interface accounting and IETF standardization. This MIB is currently supported by Junos OS for M Series and MX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-if-accounting.txt

For more information, see *Interface Accounting Forwarding Class MIB*.

- IP Forward MIB—Extends the standard IP Forwarding Table MIB (RFC 4292) to include CIDR forwarding information. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipforward.txt

For more information, see *IP Forwarding MIB*.

- IPsec Generic Flow Monitoring Object MIB—Based on **jnx-ipsec-monitor-mib**, this MIB provides support for monitoring IPsec and IPsec VPN management objects. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt

For more information, see *IPsec Generic Flow Monitoring Object MIB*.

- IPsec Monitoring MIB—Provides operational and statistical information related to the IPsec and IKE tunnels on Juniper Networks routers. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt

For more information, see *IPSec Monitoring MIB*.

- **IPsec VPN Objects MIB**—Provides support for monitoring IPsec and IPsec VPN management objects for Juniper security product lines. This MIB is an extension of **jnx-ipsec-flow-mon.mib**. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt
For more information, see *IPsec VPN Objects MIB*.
- **IPv4 MIB**—Provides additional Internet Protocol version 4 (IPv4) address information, supporting the assignment of identical IPv4 addresses to separate interfaces. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipv4.txt
For more information, see *IPv4 MIB*.
- **IPv6 and ICMPv6 MIB**—Provides IPv6 and Internet Control Message Protocol version 6 (ICMPv6) statistics. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipv6.txt
For more information, see *IPv6 MIB*.
- **L2ALD MIB**—Contains information about the Layer 2 Address Learning Daemon (L2ALD) and related traps, such as the routing instance MAC limit trap and the interface MAC limit trap. This MIB also provides VLAN information in the **jnxL2aldVlanTable** table for Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches.



NOTE: Non-ELS EX Series switches use the VLAN MIB (**jnxExVlanTable**) for VLAN information instead of this MIB. For details, see *VLAN MIB*.

For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2ald.txt

For more information, see *L2ALD MIB*.

- **L2CP MIB**—Provides information about Layer 2 Control Protocols (L2CP) based features on MX Series 3D Universal Edge Routers. Currently, Junos OS supports only the **jnxDot1dStpPortRootProtectEnabled**, **jnxDot1dStpPortRootProtectState**, and **jnxPortRootProtectStateChangeTrap** objects. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2cp-features.txt
For more information, see *L2CP MIB*.
- **L2TP MIB**—Provides information about Layer 2 Transport Protocol (L2TP) tunnels and sessions. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2tp.txt
For more information, see *L2TP MIB*.
- **LDP MIB**—Provides LDP statistics and defines LDP label-switched path (LSP) notifications. LDP traps support only IPv4 standards. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ldp.txt

For more information, see *LDP MIB*.

- License MIB—Extends SNMP support to licensing information, and introduces SNMP traps that alert users when the licenses are about to expire, expire, or when the total number of users exceeds the number specified in the license. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-license.txt

For more information, see *License MIB*.

- Logical Systems MIBs—Extend SNMP support to logical systems security profile through various MIBs defined under **jnxLsysSecurityProfile**. For downloadable versions of the MIBs, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt

For more information, see *Logical Systems MIB*.

- MIMSTP MIB—Provides information about MSTP instances (that is, routing instances of type Virtual Switch/Layer 2 control, also known as virtual contexts), MSTIs within the MSTP instance, and VLANs associated with the MSTI. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mimstp.txt

For more information, see *MIMSTP MIB*.

- MPLS MIB—Provides MPLS information and defines MPLS notifications. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mpls.txt



NOTE: To collect information about MPLS statistics on transit routers, use the enterprise-specific RSVP MIB (**mib-jnx-rsvp.txt**) instead of the enterprise-specific MPLS MIB (**mib-jnx-mpls.txt**).

For more information, see *MPLS MIB*.

- MPLS LDP MIB—Contains object definitions as described in RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mpls-ldp.txt



NOTE: Objects in the MPLS LDP MIB were supported in earlier releases of Junos OS as a proprietary LDP MIB (**mib-ldpmib.txt**). Because the branch used by the proprietary LDP (**mib-ldpmib.txt**) conflicts with RFC 3812, the proprietary LDP MIB (**mib-ldpmib.txt**) has been deprecated and replaced by the enterprise-specific MPLS LDP MIB (**mib-jnx-mpls-ldp.txt**).

For more information, see *MPLS LDP MIB*.

- MVPN MIB—Contains objects that enable SNMP manager to monitor MVPN connections on the provider edge routers. The enterprise-specific MVPN MIB is the Juniper Networks extension of the IETF standard MIBs defined in Internet draft

draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mvpn.txt.

For a downloadable version of the table in the Juniper Networks enterprise-specific L2L3-VPN-MCAST MIB that is supported in the MVPN MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2l3vpn-mcast.txt.

For more information, see *MVPN MIB*.

- NAT Objects MIB—Provides support for monitoring network address translation (NAT). This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-nat.txt

For more information, see *NAT Objects MIB*.

- NAT Resources-Monitoring MIB—Provides support for monitoring NAT pools usage and NAT rules. Notifications of usage of NAT resources are also provided by this MIB. This MIB is currently supported on the Multiservices PIC and Multiservices DPC on M Series and MX Series routers only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sp-nat.txt

For more information, see *Network Address Translation Resources—Monitoring MIB*.

- OTN Interface Management MIB—Defines objects for managing Optical Transport Network (OTN) interfaces on devices running Junos OS. For a downloadable version of the MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-otn.txt

For more information, see *OTN Interface Management MIB*.

- Packet Forwarding Engine MIB—Provides notification statistics for Packet Forwarding Engines. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pfe.txt

For more information, see *Packet Forwarding Engine MIB*.

- Packet Mirror MIB—Enables you to capture and view packet mirroring-related information. This MIB is currently supported by Junos OS for MX Series routers only. Packet mirroring traps are an extension of the standard SNMP implementation and are only available to SNMPv3 users. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-packet-mirror.txt

For more information, see *Packet Mirror MIB Overview*.

- PAE Extension MIB—Extends the standard IEEE802.1x PAE Extension MIB, and contains information for Static MAC Authentication. The enterprise-specific PAE Extension MIB is supported only on EX Series Ethernet Switches. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pae-extension.txt

For more information, see *PAE Extension MIB*.

- Passive Monitoring MIB—Performs traffic flow monitoring and lawful interception of packets transiting between two routers. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pmon.txt

For more information, see *Passive Monitoring MIB*.

- Ping MIB—Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in **pingCtlTable** of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ping.txt

For more information, see *PING MIB*.

- Policy Objects MIB—Provides support for monitoring the security policies that control the flow of traffic from one zone to another. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-policy.txt

For more information, see *Policy Objects MIB*.

- Power Supply Unit MIB—Enables monitoring and managing of the power supply on a device running Junos OS. This MIB is currently supported only on EX Series Ethernet Switches. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-power-supply-unit.txt

For more information, see *Power Supply Unit MIB*.

- PPP MIB—Provides SNMP support for PPP-related information such as the type of authentication used, interface characteristics, status, and statistics. This MIB is supported on Common Edge PPP process, jpppd. This MIB is currently supported only on M Series and MX Series routers. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ppp.txt

For more information, see *PPP MIB*.

- PPPoE MIB—Provides SNMP support for PPPoE-related information such as the type of authentication used, interface characteristics, status, and statistics. This MIB is supported on Common Edge PPPoE process, jpppoed. This MIB is currently supported only on M Series and MX Series routers. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pppoe.txt

For more information, see *PPPoE MIB*.

- Pseudowire TDM MIB—Extends the standard Pseudowire MIB, and contains information about configuration and statistics for specific pseudowire types. The enterprise-specific Pseudowire TDM MIB is the Juniper Networks implementation of the standard Managed Objects for TDM over Packet Switched Network MIB (draft-ietf-pwe3-tdm-mib-08.txt). For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pwtdm.txt

For more information, see *Pseudowire TDM MIB*.

- Pseudowire ATM MIB—Extends the standard Pseudowire MIB, and defines objects used for managing the ATM pseudowires in Juniper products. The enterprise-specific Pseudowire ATM MIB is the Juniper Networks implementation of RFC 5605, *Managed Objects for ATM over Packet Switched Networks (PSNs)*. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pwatm.txt

For more information, see *Pseudowire ATM MIB*.

- PTP MIB—Monitors the operation of PTP clocks within the network. This MIB is currently supported by Junos OS for MX Series routers only. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-timing-notifications.txt

For more information, see *PTP MIB*.

- Real-Time Performance Monitoring MIB—Provides real-time performance-related data and enables you to access jitter measurements and calculations using SNMP. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rpm.txt

For more information, see *Real-Time Performance Monitoring MIB*.

- Reverse-Path-Forwarding MIB—Monitors statistics for traffic that is rejected because of reverse-path-forwarding (RPF) processing. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rpf.txt



NOTE: The enterprise-specific RPF MIB is not supported on EX Series Ethernet Switches.

For more information, see *Reverse Path Forwarding MIB*.

- RMON Events and Alarms MIB—Supports the Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments **alarmTable** with additional information about each alarm. Two new traps are also defined to indicate when problems are encountered with an alarm. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rmon.txt

For more information, see *RMON Events and Alarms MIB*.

- RSVP MIB—Provides information about RSVP-traffic engineering sessions that correspond to MPLS LSPs on transit routers in the service provider core network. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rsvp.txt



NOTE: To collect information about MPLS statistics on transit routers, use the enterprise-specific RSVP MIB (**mib-jnx-rsvp.txt**) instead of the enterprise-specific MPLS MIB (**mib-jnx-mpls.txt**).

For more information, see *RSVP MIB*.

- Security Interface Extension Objects MIB—Provides support for the security management of interfaces. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-if-ext.txt

For more information, see *Security Interface Extension Objects MIB*.

- Security Screening Objects MIB—Defines the MIB for the Juniper Networks Enterprise Firewall screen functionality. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-screening.txt
For more information, see *Security Screening Objects MIB*.
- Services PIC MIB—Provides statistics for Adaptive Services (AS) PICs and defines notifications for AS PICs. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sp.txt
For more information, see *Services PIC MIB*.
- SONET APS MIB—Monitors any SONET interface that participates in Automatic Protection Switching (APS). For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sonetaps.txt
For more information, see *SONET APS MIB*.
- SONET/SDH Interface Management MIB—Monitors the current alarm for each SONET/SDH interface. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sonet.txt
For more information, see *SONET/SDH Interface Management MIB*.
- Source Class Usage MIB—Counts packets sent to customers by performing a lookup on the IP source address and the IP destination address. The Source Class Usage (SCU) MIB makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-scu.txt
For more information, see *Source Class Usage MIB*.
- SPU Monitoring MIB—Provides support for monitoring SPUs on SRX5600 and SRX5800 devices. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt
For more information, see *SPU Monitoring Objects MIB*.
- Structure of Management Information MIB—Explains how the Juniper Networks enterprise-specific MIBs are structured. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-smi.txt
For more information, see *Structure of Management Information MIB*.
- Structure of Management Information MIB for EX Series Ethernet Switches—Defines a MIB branch for switching-related MIB definitions for the EX Series Ethernet Switches. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ex-smi.txt
For more information, see *EX Series SMI MIB*.
- Structure of Management Information MIB for SRX Series —Contains object identifiers (OIDs) for the security branch of the MIBs used in Junos OS for SRX Series devices, services, and traps. This MIB is currently supported by Junos OS for SRX Series devices

only. For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-smi.txt

For more information, see *Structure of Management Information MIB*.

- Subscriber MIB—Provides SNMP support for subscriber-related information. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-subscriber.txt

For more information, see *Subscriber MIB*.

- System Log MIB—Enables notification of an SNMP trap-based application when an important system log message occurs. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-syslog.txt

For more information, see *System Log MIB*.

- Traceroute MIB—Supports the Junos OS extensions of traceroute and remote operations. Items in this MIB are created when entries are created in the **traceRouteCtlTable** of the Traceroute MIB. Each item is indexed exactly the same way as it is in the Traceroute MIB. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-traceroute.txt

For more information, see *Traceroute MIB*.

- Utility MIB—Provides SNMP support for exposing the Junos OS data and has tables that contain information about each type of data, such as integer and string. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-util.txt

For more information, see *Utility MIB*.

- Virtual Chassis MIB—Contains information about the virtual chassis on the EX Series Ethernet Switches and the MX Series. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-virtualchassis.txt

For more information, see *Virtual Chassis MIBs*.

- VLAN MIB—Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients. The enterprise-specific VLAN MIB is supported only on EX Series Ethernet Switches.



NOTE: For ELS EX Series switches and QFX Series switches, VLAN information is available in the L2ALD MIB in the **jnxL2aldVlanTable** table instead of in the VLAN MIB. See *L2ALD MIB* for details. For non-ELS EX Series switches, VLAN information is provided in the VLAN MIB in the **jnxExVlanTable** table.

For a downloadable version of this MIB, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vlan.txt

For more information, see *VLAN MIB*.

- VPLS MIBs—Provides information about generic, BGP-based, and LDP-based VPLS and pseudowires associated with the VPLS networks. The enterprise-specific VPLS

MIBs are Juniper Networks extensions of the following IETF standard MIBs defined in Internet draft draft-ietf-l2vpn-vpls-mib-05.txt, and are implemented as part of the `jnxExperiment` branch:

- **VPLS-Generic-Draft-01-MIB** implemented as `mib-jnx-vpls-generic.txt`
- **VPLS-BGP-Draft-01-MIB** implemented as `mib-jnx-vpls-bgp.txt`
- **VPLS-LDP-Draft-01-MIB** implemented as `mib-jnx-vpls-ldp.txt`

For downloadable versions of these MIBs, see:

- http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-generic.txt
- http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-bgp.txt
- http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-ldp.txt

For more information, see *Interpreting the Enterprise-Specific VPLS MIBs*.

- **VPN Certificate Objects MIB**—Provides support for monitoring the local and CA certificates loaded on the router. This MIB is currently supported by Junos OS for SRX Series devices only. For a downloadable version of this MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-cert.txt

For more information, see *VPN Certificate Objects MIB*.

- **VPN MIB**—Provides monitoring for Layer 3 VPNs, Layer 2 VPNs, and virtual private LAN service (VPLS) (read access only). For a downloadable version of the MIB, see http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpn.txt

For more information, see *VPN MIB*.

Related Documentation

- [Standard SNMP MIBs Supported by Junos OS on page 1409](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1439](#)
- [Loading MIB Files to a Network Management System on page 1459](#)

Enterprise-Specific MIBs and Supported Devices

Table 112 lists the enterprise-specific MIBs that are supported on various devices running the Junos OS.



NOTE: In this table, a value of 1 in any of the platform columns (ACX, M, MX, T, EX, PTX, and SRX) denotes that the corresponding MIB is supported on that particular platform. A value of 0 denotes that the MIB is not supported on the platform.



NOTE: This topic uses the following classification for SRX Series devices: Low-End (SRX300, SRX320, and SRX340), Mid-Range (SRX550M), and High-End (SRX1500, SRX5400, SRX5600, and SRX5800).

Table 112: Enterprise-Specific MIBs and Supported Devices

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
AAA Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-user-aaa.txt	0	1	1	0	0	0	0	1	1
Access Authentication Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-auth.txt	0	0	0	0	1	0	1	1	1
Alarm MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chassis-alarm.txt	1	1	1	1	1	1	1	1	1
Analyzer MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-analyzer.txt	0	0	0	1	0	0	0	0	0
Antivirus Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-utm-av.txt	0	0	0	0	0	0	1	0	0
ATM Class-of-Service MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-atm-cos.txt	0	1	1	0	0	0	1	0	1
ATM MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-atm.txt	1	1	1	0	0	0	0	0	0
BGP4 V2 MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-bgpmib2.txt	1	1	1	1	1	1	1	1	1
Bidirectional Forwarding Detection MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-bfd.txt	1	1	1	1	1	1	1	1	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Chassis Forwarding MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chassis-fwdd.txt	1	0	0	0	1	1	1	0	0
Chassis MIBs http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chassis.txt http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-chas-defines.txt	1	1	1	1	1	1	1	1	1
Chassis Cluster MIBs http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jsrpd.txt	0	0	0	0	0	0	0	1	1
Class-of-Service MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-cos.txt	1	1	1	1	1	1	0	0	1
Configuration Management MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-cfgmgmt.txt	1	1	1	1	1	1	1	1	1
Destination Class Usage MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dcu.txt	0	1	1	0	1	0	0	1	1
DHCP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jdhcp.txt	0	1	1	0	0	0	0	0	0
DHCPv6 MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-jdhcpv6.txt	0	1	1	0	0	0	0	0	0
Digital Optical Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dom.txt	0	1	1	1	1	1	0	0	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
DNS Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-dns.txt	0	0	0	0	0	0	0	1	1
Dynamic Flow Capture MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-dfc.txt	0	1	1	0	0	0	0	0	0
Ethernet MAC MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/jnx-mac.txt	0	1	1	1	1	0	0	0	1
Event MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-event.txt	1	1	1	1	1	1	1	1	1
EX Series MAC Notification MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ex-mac-notification.txt	0	0	0	1	0	0	0	0	0
EX Series SMI MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ex-smi.txt	0	0	0	1	0	0	0	0	0
Experimental MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-exp.txt	1	1	1	1	1	0	0	0	0
Firewall MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-firewall.txt	1	1	1	1	1	1	1	1	1
Flow Collection Services MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-coll.txt	0	1	1	0	0	0	0	0	0

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Host Resources MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-hostresources.txt	1	1	1	1	1	0	1	1	1
Interface MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-if-extensions.txt	1	1	1	1	1	1	1	1	1
IP Forward MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipforward.txt	1	1	1	1	1	1	1	1	1
IPsec Generic Flow Monitoring Object MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt	0	0	0	0	0	0	1	1	1
IPsec Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt	0	1	1	0	1	0	0	1	0
IPsec VPN Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt	0	0	0	0	0	0	1	0	0
IPv4 MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipv4.txt	1	1	1	1	1	1	1	1	1
IPv6 and ICMPv6 MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ipv6.txt	0	1	1	1	0	1	1	1	1
L2ALD MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2ald.txt	0	0	1	1	0	0	0	0	0

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
L2CP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2cp-features.txt	0	0	0	1	0	0	0	0	0
L2TP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2tp.txt	0	1	1	0	0	0	0	0	0
LDP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ldp.txt	1	1	1	0	0	1	0	0	1
License MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-license.txt	0	1	1	0	0	0	1	1	1
Logical Systems MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt	0	0	0	0	0	0	0	1	1
MIMSTP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mimstp.txt	0	0	1	1	0	0	0	0	0
MPLS LDP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mpls-ldp.txt	1	1	1	1	1	1	0	0	0
MPLS MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mpls.txt	1	1	1	1	1	1	0	0	1
MVPN MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-mvpn.txt and http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-l2l3vpn-mcast.txt	1	1	1	1	1	1	1	1	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
NAT Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-nat.txt	0	0	0	0	1	0	1	1	1
NAT Resources-Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sp-nat.txt	0	1	1	0	0	0	0	0	0
OTN Interface Management MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-otn.txt	0	1	1	0	0	0	0	0	0
Packet Forwarding Engine MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pfe.txt	1	1	1	0	1	1	1	1	1
Packet Mirror MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-packet-mirror.txt	0	0	0	1	0	0	0	0	0
PAE Extension MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pae-extension.txt	0	0	0	1	0	0	0	0	0
Passive Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pmon.txt	0	1	1	0	0	0	0	0	0
Ping MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ping.txt	1	1	1	1	1	0	1	1	1
Policy Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-policy.txt	0	0	0	0	1	0	1	1	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Power Supply Unit MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-power-supply-unit.txt	0	0	0	1	0	1	0	0	0
PPP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-ppp.txt	0	1	1	0	0	0	0	0	0
PPPoE MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pppoe.txt	0	1	1	0	0	0	0	0	0
Pseudowire ATM MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pwatm.txt	0	1	0	1	0	0	0	0	0
Pseudowire TDM MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-pwtdm.txt	1	1	1	0	0	0	0	0	0
PTP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-timing-notifications.txt	0	0	0	1	0	0	0	0	0
Real-Time Performance Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rpm.txt	0	1	1	1	1	0	1	0	0
Reverse-Path-Forwarding MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rpf.txt	1	1	1	1	1	1	1	1	1
RMON Events and Alarms MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rmon.txt	1	1	1	1	1	1	1	1	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
RSVP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-rsvp.txt	1	1	1	1	0	1	0	0	0
Security Interface Extension Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-if-ext.txt	0	0	0	0	1	0	1	1	1
Security Screening Objects MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-screening.txt	0	0	0	0	0	0	0	0	1
Services PIC MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sp.txt	0	1	1	0	0	0	0	0	0
SNMP IDP MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-idp.txt	0	0	0	0	0	0	1	1	0
SONET APS MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sonetaps.txt	0	1	1	0	0	0	0	0	0
SONET/SDH Interface Management MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-sonet.txt	0	1	1	0	0	0	0	0	0
Source Class Usage MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-scu.txt	0	1	1	0	0	0	0	0	1
SPU Monitoring MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt	0	0	0	0	0	0	1	1	1

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
Structure of Management Information MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-smi.txt	1	1	1	1	1	0	1	1	1
Subscriber MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-subscriber.txt	1	0	1	0	0	0	0	0	0
System Log MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-syslog.txt	0	1	1	1	1	1	1	1	1
Traceroute MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-traceroute.txt	0	1	1	1	1	0	1	1	1
Utility MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-util.txt	0	1	1	1	1	0	1	1	1
Virtual Chassis MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-virtualchassis.txt	0	0	0	1	1	0	0	0	0
VLAN MIB http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vlan.txt	0	0	0	1	0	0	0	0	0
VPLS MIBs <ul style="list-style-type: none"> http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-generic.txt http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-ldp.txt http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpls-bgp.txt 	0	1	1	1	0	0	0	0	0

Table 112: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms								
	ACX	M	T	MX	EX	PTX	SRX		
							Low-End	Mid-Range	High-End
VPN Certificate Objects MIB	0	0	0	0	1	0	1	1	1
http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-js-cert.txt									
VPN MIB	1	1	1	1	1	0	0	0	0
http://www.juniper.net/techpubs/en_US/junos15.1/topics/reference/mibs/mib-jnx-vpn.txt									

Related Documentation

- Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427
- Juniper Networks Enterprise-Specific SNMP Traps on page 1456
- Standard SNMP MIBs Supported by Junos OS on page 1409
- Loading MIB Files to a Network Management System on page 1459

SNMP MIB Objects Supported by Junos OS for the SNMP Set Operation

The following table lists the SNMP MIB objects that are supported for the **snmp set** operation by Junos OS.

Object Name	Object Identifier
RFC 1907	
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
snmpEnableAuthenTraps	1.3.6.1.2.1.1.30
RFC 2819a	
alarmInterval	1.3.6.1.2.1.16.3.1.1.2
alarmVariable	1.3.6.1.2.1.16.3.1.1.2
alarmSampleType	1.3.6.1.2.1.16.3.1.1.4

Object Name	Object Identifier
alarmStartupAlarm	1.3.6.1.2.1.16.3.1.1.6
alarmRisingThreshold	1.3.6.1.2.1.16.3.1.1.7
alarmFallingThreshold	1.3.6.1.2.1.16.3.1.1.8
alarmRisingEventIndex	1.3.6.1.2.1.16.3.1.1.9
alarmFallingEventIndex	1.3.6.1.2.1.16.3.1.1.10
alarmOwner	1.3.6.1.2.1.16.3.1.1.11
alarmStatus	1.3.6.1.2.1.16.3.1.1.12
eventDescription	1.3.6.1.2.1.16.9.1.1.2
eventType	1.3.6.1.2.1.16.9.1.1.3
eventCommunity	1.3.6.1.2.1.16.9.1.1.4
eventOwner	1.3.6.1.2.1.16.9.1.1.6
eventStatus	1.3.6.1.2.1.16.9.1.1.7
RFC 2925a	
pingMaxConcurrentRequests	1.3.6.1.2.1.80.1.1
pingCtlTargetAddressType	1.3.6.1.2.1.80.1.2.1.3
pingCtlTargetAddress	1.3.6.1.2.1.80.1.2.1.4
pingCtlDataSize	1.3.6.1.2.1.80.1.2.1.5
pingCtlTimeOut	1.3.6.1.2.1.80.1.2.1.6
pingCtlProbeCount	1.3.6.1.2.1.80.1.2.1.7
pingCtlAdminStatus	1.3.6.1.2.1.80.1.2.1.8
pingCtlDataFill	1.3.6.1.2.1.80.1.2.1.9
pingCtlFrequency	1.3.6.1.2.1.80.1.2.1.10
pingCtlMaxRows	1.3.6.1.2.1.80.1.2.1.11
pingCtlStorageType	1.3.6.1.2.1.80.1.2.1.12

Object Name	Object Identifier
pingCtlTrapGeneration	1.3.6.1.2.1.80.1.2.1.13
pingCtlTrapProbeFailureFilter	1.3.6.1.2.1.80.1.2.1.14
pingCtlTrapTestFailureFilter	1.3.6.1.2.1.80.1.2.1.15
pingCtlType	1.3.6.1.2.1.80.1.2.1.16
pingCtlDescr	1.3.6.1.2.1.80.1.2.1.17
pingCtlSourceAddressType	1.3.6.1.2.1.80.1.2.1.18
pingCtlSourceAddress	1.3.6.1.2.1.80.1.2.1.19
pingCtlIfIndex	1.3.6.1.2.1.80.1.2.1.20
pingCtlByPassRouteTable	1.3.6.1.2.1.80.1.2.1.21
pingCtlDSField	1.3.6.1.2.1.80.1.2.1.22
pingCtlRowStatus	1.3.6.1.2.1.80.1.2.1.23
RFC 2925B	
traceRouteMaxConcurrentRequests	1.3.6.1.2.1.81.1.1
traceRouteCtlTargetAddressType	1.3.6.1.2.1.81.1.2.1.3
traceRouteCtlTargetAddress	1.3.6.1.2.1.81.1.2.1.4
traceRouteCtlByPassRouteTable	1.3.6.1.2.1.81.1.2.1.5
traceRouteCtlDataSize	1.3.6.1.2.1.81.1.2.1.6
traceRouteCtlTimeOut	1.3.6.1.2.1.81.1.2.1.7
traceRouteCtlProbesPerHop	1.3.6.1.2.1.81.1.2.1.8
traceRouteCtlPort	1.3.6.1.2.1.81.1.2.1.9
traceRouteCtlMaxTtl	1.3.6.1.2.1.81.1.2.1.10
traceRouteCtlDSField	1.3.6.1.2.1.81.1.2.1.11
traceRouteCtlSourceAddressType	1.3.6.1.2.1.81.1.2.1.12
traceRouteCtlSourceAddress	1.3.6.1.2.1.81.1.2.1.13

Object Name	Object Identifier
traceRouteCtlIfIndex	1.3.6.1.2.1.81.1.2.1.14
traceRouteCtlMiscOptions	1.3.6.1.2.1.81.1.2.1.15
traceRouteCtlMaxFailure	1.3.6.1.2.1.81.1.2.1.16
traceRouteCtlDontFragment	1.3.6.1.2.1.81.1.2.1.17
traceRouteCtlInitialTtl	1.3.6.1.2.1.81.1.2.1.18
traceRouteCtlFrequency	1.3.6.1.2.1.81.1.2.1.19
traceRouteCtlStorageType	1.3.6.1.2.1.81.1.2.1.20
traceRouteCtlAdminStatus	1.3.6.1.2.1.81.1.2.1.21
traceRouteCtlDescr	1.3.6.1.2.1.81.1.2.1.22
traceRouteCtlMaxRows	1.3.6.1.2.1.81.1.2.1.23
traceRouteCtlTrapGeneration	1.3.6.1.2.1.81.1.2.1.24
traceRouteCtlCreateHopEntries	1.3.6.1.2.1.81.1.2.1.25
traceRouteCtlType	1.3.6.1.2.1.81.1.2.1.26
traceRouteCtlRowStatus	1.3.6.1.2.1.81.1.2.1.27
Enterprise-Specific PING MIB	
jnxPingCtlIfName	1.3.6.1.4.1.2636.3.7.1.2.1.3
jnxPingCtlRoutingIfIndex	1.3.6.1.4.1.2636.3.7.1.2.1.4
jnxPingCtlRoutingIfName	1.3.6.1.4.1.2636.3.7.1.2.1.5
jnxPingCtlRoutingInstanceName	1.3.6.1.4.1.2636.3.7.1.2.1.6
jnxPingCtlRttThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.7
jnxPingCtlRttStdDevThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.8
jnxPingCtlRttJitterThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.9
jnxPingCtlEgressTimeThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.10
jnxPingCtlEgressStdDevThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.11

Object Name	Object Identifier
jnxPingCtlEgressJitterThreshold	1.3.6.1.4.1.2636.3.71.2.1.12
jnxPingCtlIngressTimeThreshold	1.3.6.1.4.1.2636.3.71.2.1.13
jnxPingCtlIngressStdDevThreshold	1.3.6.1.4.1.2636.3.71.2.1.14
jnxPingCtlIngressJitterThreshold	1.3.6.1.4.1.2636.3.71.2.1.15
jnxPingTrapGeneration	1.3.6.1.4.1.2636.3.71.2.1.16
Enterprise-Specific Traceroute MIB	
jnxTRCtlIfName	1.3.6.1.4.1.2636.3.8.1.2.1.3
jnxTRCtlRoutingInstanceName	1.3.6.1.4.1.2636.3.8.1.2.1.4
RFC 3413 Target MIB	
snmpTargetSpinLock	1.3.6.1.6.3.12.1.1
snmpTargetAddrTDomain	1.3.6.1.6.3.12.1.2.1.2
snmpTargetAddrTAddress	1.3.6.1.6.3.12.1.2.1.3
snmpTargetAddrTimeout	1.3.6.1.6.3.12.1.2.1.4
snmpTargetAddrRetryCount	1.3.6.1.6.3.12.1.2.1.5
snmpTargetAddrTagList	1.3.6.1.6.3.12.1.2.1.6
snmpTargetAddrParams	1.3.6.1.6.3.12.1.2.1.7
snmpTargetAddrStorageType	1.3.6.1.6.3.12.1.2.1.8
snmpTargetAddrRowStatus	1.3.6.1.6.3.12.1.2.1.9
snmpTargetParamsMPModel	1.3.6.1.6.3.12.1.3.1.2
snmpTargetParamsSecurityModel	1.3.6.1.6.3.12.1.3.1.3
snmpTargetParamsSecurityLevel	1.3.6.1.6.3.12.1.3.1.4
snmpTargetParamsSecurityName	1.3.6.1.6.3.12.1.3.1.5
snmpTargetParamsStorageType	1.3.6.1.6.3.12.1.3.1.6
snmpTargetParamsRowStatus	1.3.6.1.6.3.12.1.3.1.7

Object Name	Object Identifier
RFC 3413 Notify MIB	
snmpNotifyTag	1.3.6.1.6.3.13.1.1.1.2
snmpNotifyType	1.3.6.1.6.3.13.1.1.1.3
snmpNotifyStorageType	1.3.6.1.6.3.13.1.1.1.4
snmpNotifyRowStatus	1.3.6.1.6.3.13.1.1.1.5
snmpNotifyFilterProfileName	1.3.6.1.6.3.13.1.2.1.1
snmpNotifyFilterProfileStorType	1.3.6.1.6.3.13.1.2.1.2
snmpNotifyFilterProfileRowStatus	1.3.6.1.6.3.13.1.2.1.3
snmpNotifyFilterMask	1.3.6.1.6.3.13.1.3.1.2
snmpNotifyFilterType	1.3.6.1.6.3.13.1.3.1.3
snmpNotifyFilterStorageType	1.3.6.1.6.3.13.1.3.1.4
snmpNotifyFilterRowStatus	1.3.6.1.6.3.13.1.3.1.5
RFC 2574	
usmUserSpinLock	1.3.6.1.6.3.15.1.2.1
usmUserCloneFrom	1.3.6.1.6.3.15.1.2.2.1.4
usmUserAuthProtocol	1.3.6.1.6.3.15.1.2.2.1.5
usmUserAuthKeyChange	1.3.6.1.6.3.15.1.2.2.1.6
usmUserOwnAuthKeyChange	1.3.6.1.6.3.15.1.2.2.1.7
usmUserPrivProtocol	1.3.6.1.6.3.15.1.2.2.1.8
usmUserPrivKeyChange	1.3.6.1.6.3.15.1.2.2.1.9
usmUserOwnPrivKeyChange	1.3.6.1.6.3.15.1.2.2.1.10
usmUserPublic	1.3.6.1.6.3.15.1.2.2.1.11
usmUserStorageType	1.3.6.1.6.3.15.1.2.2.1.12
usmUserStatus	1.3.6.1.6.3.15.1.2.2.1.13

Object Name	Object Identifier
RFC 2575	
vacmGroupName	1.3.6.1.6.3.16.1.2.1.3
vacmSecurityToGroupStorageType	1.3.6.1.6.3.16.1.2.1.4
vacmSecurityToGroupStatus	1.3.6.1.6.3.16.1.2.1.5
vacmAccessContextMatch	1.3.6.1.6.3.16.1.4.1.4
vacmAccessReadViewName	1.3.6.1.6.3.16.1.4.1.5
vacmAccessWriteViewName	1.3.6.1.6.3.16.1.4.1.6
vacmAccessNotifyViewName	1.3.6.1.6.3.16.1.4.1.7
vacmAccessStorageType	1.3.6.1.6.3.16.1.4.1.8
vacmAccessStatus	1.3.6.1.6.3.16.1.4.1.9
vacmViewSpinLock	1.3.6.1.6.3.16.1.5.1
vacmViewTreeFamilyMask	1.3.6.1.6.3.16.1.5.2.1.3
vacmViewTreeFamilyType	1.3.6.1.6.3.16.1.5.2.1.4
vacmViewTreeFamilyStorageType	1.3.6.1.6.3.16.1.5.2.1.5
vacmViewTreeFamilyStatus	1.3.6.1.6.3.16.1.5.2.1.6
RFC 2576	
snmpCommunityName	1.3.6.1.6.3.18.1.1.1.2
snmpCommunitySecurityName	1.3.6.1.6.3.18.1.1.1.3
snmpCommunityContextEngineID	1.3.6.1.6.3.18.1.1.1.4
snmpCommunityContextName	1.3.6.1.6.3.18.1.1.1.5
snmpCommunityTransportTag	1.3.6.1.6.3.18.1.1.1.6
snmpCommunityStorageType	1.3.6.1.6.3.18.1.1.1.7
snmpCommunityStatus	1.3.6.1.6.3.18.1.1.1.8
RFC 2576	

Object Name	Object Identifier
snmpTargetAddrMask	1.3.6.1.6.3.18.1.2.1.1
snmpTargetAddrMMS	1.3.6.1.6.3.18.1.2.1.2

**Related
Documentation**

- [Standard SNMP MIBs Supported by Junos OS on page 1409](#)
- [Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1439](#)

Standard SNMP Traps Supported on Devices Running Junos OS

This topic provides pointers to the standard SNMP traps supported by the Junos OS.



NOTE: For scalability reasons, the MPLS traps are generated by the ingress router only.

- *Standard SNMP Version 1 Traps*
- *Standard SNMP Version 2 Traps*
- *Standard SNMP Traps on EX Series Ethernet Switches*
- *Unsupported Standard SNMP Traps*

**Related
Documentation**

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1456](#)
- [Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1409](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
- *Managing Traps and Informs*

Juniper Networks Enterprise-Specific SNMP Traps

This topic provides pointers to the enterprise-specific SNMP traps supported by the Junos OS.



NOTE: All enterprise-specific SNMP traps supported by the Junos OS can be sent in version 1, 2, and 3 formats.

- *Juniper Networks Enterprise-Specific SNMP Version 1 Traps*
- *Juniper Networks Enterprise-Specific SNMP Version 2 Traps*
- *Juniper Networks Enterprise-Specific BGP Traps*

- *Juniper Networks Enterprise-Specific DOM Traps*
- *Juniper Networks Enterprise-Specific LDP Traps*
- *Juniper Networks Enterprise-Specific License MIB Notifications*
- *Juniper Networks Enterprise-Specific MIMSTP Traps*
- *Juniper Networks Enterprise-Specific MPLS Traps*



NOTE: For scalability reasons, the MPLS traps are generated by the ingress router only. For information about disabling the generation of MPLS traps, see the Junos OS MPLS Applications Feature Guide for Routing Devices.

**Related
Documentation**

- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1456](#)
- [Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1409](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
- *Managing Traps and Informs*

Loading MIB Files to a Network Management System

- Loading MIB Files to a Network Management System on page 1459

Loading MIB Files to a Network Management System

For your network management system (NMS) to identify and understand the MIB objects used by the Junos OS, you must first load the MIB files to your NMS using a MIB compiler. A MIB compiler is a utility that parses the MIB information such as the MIB object name, IDs, and data type for the NMS.

You can download the Junos MIB package from the Junos OS Enterprise MIBs index at http://www.juniper.net/techpubs/en_US/release-independent/junos/mibs/mibs.html. The Junos MIB package is available in **.zip** and **.tar** packages. You can download the appropriate format based on your requirements.

The Junos MIB package contains two folders: **StandardMibs** and **JuniperMibs**. The **StandardMibs** folder contains the standard MIBs and RFCs that are supported on devices running the Junos OS, whereas the **JuniperMibs** folder contains the Juniper Networks enterprise-specific MIBs.

To load MIB files that are required for managing and monitoring devices running the Junos OS:

1. Go to the Junos OS Enterprise MIBs index page (http://www.juniper.net/techpubs/en_US/release-independent/junos/mibs/mibs.html).
2. Click the **TAR** or **ZIP** link under the appropriate release heading to download the Junos MIB package for that release.
3. Decompress the file (**.tar** or **.zip**) using an appropriate utility.
4. Load the standard MIB files (from the **StandardMibs** folder) in the following order:



NOTE: Some of the MIB compilers that are commonly used have the standard MIBs preloaded on them. If the standard MIBs are already loaded on the MIB compiler that you are using, skip this step and proceed to Step 7.

- a. `mib-SNMPv2-SMI.txt`
- b. `mib-SNMPv2-TC.txt`
- c. `mib-IANAifType-MIB.txt`
- d. `mib-IANA-RTPROTO-MIB.txt`
- e. `mib-rfc1907.txt`
- f. `mib-rfc2011a.txt`
- g. `mib-rfc2012a.txt`
- h. `mib-rfc2013a.txt`
- i. `mib-rfc2863a.txt`

5. Load the remaining standard MIB files.



NOTE: You must follow the order specified in this procedure, and ensure that all standard MIBs are loaded before you load the enterprise-specific MIBs. There might be dependencies that require a particular MIB to be present on the compiler before loading some other MIB. You can find such dependencies listed in the **IMPORT** section of the MIB file.

6. Load the Juniper Networks enterprise-specific SMI MIB, `mib-jnx-smi.txt`, and the following optional SMI MIBs based on your requirements:

- `mib-jnx-js-smi.txt`—(Optional) For Juniper Security MIB tree objects
- `mib-jnx-ex-smi.txt`—(Optional) For EX Series Ethernet Switches
- `mib-jnx-exp.txt`—(Recommended) For Juniper Networks experimental MIB objects

7. Load the remaining enterprise-specific MIBs from the **JuniperMibs** folder.



TIP: While loading a MIB file, if the compiler returns an error message saying that any of the objects is undefined, open the MIB file using a text editor and ensure that all the MIB files listed in the **IMPORT** section are loaded on the compiler. If any of the MIB files listed in the **IMPORT** section is not loaded on the compiler, load that MIB file, and then try to load the MIB file that failed to load.

For example, the enterprise-specific PING MIB, `mib-jnx-ping.txt`, has dependencies on RFC 2925, DiSMAN-PING-MIB, `mib-rfc2925a.txt`. If you try to load `mib-jnx-ping.txt` before loading `mib-rfc2925a.txt`, the compiler returns an error message saying that certain objects in `mib-jnx-ping.txt` are undefined. Load `mib-rfc2925a.txt`, and then try to load `mib-jnx-ping.txt`. The enterprise-specific PING MIB, `mib-jnx-ping.txt`, then loads without any issue.

Related Documentation

- [Standard SNMP MIBs Supported by Junos OS on page 1409](#)

- [Enterprise-Specific SNMP MIBs Supported by Junos OS on page 1427](#)

CHAPTER 63

Configuring SNMP

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
- [Optimizing the Network Management System Configuration for the Best Results on page 1467](#)
- [Configuring Options on Managed Devices for Better SNMP Response Time on page 1469](#)
- [Configuring SNMP on Devices Running Junos OS on page 1471](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1474](#)
- [Configuring the System Location for a Device Running Junos OS on page 1475](#)
- [Configuring the System Description on a Device Running Junos OS on page 1475](#)
- [Configuring SNMP Details on page 1476](#)
- [Configuring a Different System Name on page 1477](#)
- [Configuring the Commit Delay Timer on page 1478](#)
- [Filtering Duplicate SNMP Requests on page 1478](#)
- [Configuring SNMP Communities on page 1479](#)
- [Examples: Configuring the SNMP Community String on page 1482](#)
- [Adding a Group of Clients to an SNMP Community on page 1482](#)
- [Configuring a Proxy SNMP Agent on page 1484](#)
- [Configuring SNMP Traps on page 1485](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
- [Configuring SNMP Trap Options on page 1487](#)
- [Configuring SNMP Trap Groups on page 1491](#)
- [Example: Configuring SNMP Trap Groups on page 1493](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1494](#)
- [Example: Configuring Secured Access List Checking on page 1494](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1495](#)
- [Configuring MIB Views on page 1496](#)
- [Example: Ping Proxy MIB on page 1497](#)

Configuration Statements at the [edit snmp] Hierarchy Level

This topic shows all possible configuration statements at the **[edit snmp]** hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

```
[edit]
snmp {
  alarm-management {
    alarm-list-name list-name {
      alarm-id id {
        alarm-state state {
          description alarm-description;
          notification-id notification-id-of-alarm;
          resource-prefix alarm-resource-prefix;
          varbind-index varbind-index-in-alarm-varbind-list;
          varbind-subtree alarm-varbind-subtree;
          varbind-value alarm-varbind-value;
        }
      }
    }
  }
  client-list client-list-name {
    ip-addresses;
  }
  community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
      address <restrict>;
    }
    logical-system logical-system-name {
      routing-instance routing-instance-name;
      clients {
        address <restrict>;
      }
    }
    routing-instance routing-instance-name {
      clients {
        address <restrict>;
      }
    }
    view view-name;
  }
  contact contact;
  description description;
  engine-id {
    (local engine-id | use-default-ip-address | use-mac-address);
  }
  filter-duplicates;
  interface [ interface-names ];
  location location;
  name name;
```



```

nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index;
        rising-threshold integer;
        sample-type type;
        startup-alarm alarm;
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regular-expression>;
    flag flag;
    memory-trace;
    no-remote-trace;
    no-default-memory-trace;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
    logical-system logical-system-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
    enterprise-oid;
    logical-system logical-system-name {
        routing-instance routing-instance-name {
            source-address address;
        }
    }
    routing-instance routing-instance-name {
        source-address address;
    }
}

```

```
}
v3 {
  notify name {
    tag tag-name;
    type (trap | inform);
  }
  notify-filter profile-name {
    oid oid (include | exclude);
  }
  snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
  }
  target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    retry-count number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | v3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
}
usm {
  local-engine {
    user username {
      authentication-md5 {
        authentication-password authentication-password;
      }
      authentication-none;
      authentication-sha {
        authentication-password authentication-password;
      }
      privacy-3des {
        privacy-password privacy-password;
      }
      privacy-aes128 {
        privacy-password privacy-password;
      }
      privacy-des {
        privacy-password privacy-password;
      }
      privacy-none;
    }
  }
}
```

```

}
vacm {
  access {
    group group-name {
      (default-context-prefix | context-prefix context-prefix){
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}
view view-name {
  oid object-identifier (include | exclude);
}
}

```

- Related Documentation**
- [Understanding the SNMP Implementation in Junos OS](#)
 - [Configuring SNMP on a Device Running Junos OS](#)

Optimizing the Network Management System Configuration for the Best Results

You can modify your network management system configuration to optimize the response time for SNMP queries. The following sections contain a few tips on how you can configure the network management system:

- [Changing the Polling Method from Column-by-Column to Row-by-Row on page 1467](#)
- [Reducing the Number of Variable Bindings per PDU on page 1468](#)
- [Increasing Timeout Values in Polling and Discovery Intervals on page 1468](#)
- [Reducing Incoming Packet Rate at the snmpd on page 1468](#)

Changing the Polling Method from Column-by-Column to Row-by-Row

You can configure the network management system to use the row-by-row method for SNMP data polling. It has been proven that the row-by-row and multiple row-by-multiple-row polling methods are more efficient than column-by-column polling. By configuring the network management system to use the row-by-row data polling method, you can ensure that data for only one interface is polled in a request instead of

a single request polling data for multiple interfaces, as is the case with column-by-column polling. Row-by-row polling also reduces the risk of requests timing out.

Reducing the Number of Variable Bindings per PDU

By reducing the number of variable bindings per protocol data unit (PDU), you can improve the response time for SNMP requests. A request that polls for data related to multiple objects, which are mapped to different index entries, translates into multiple requests at the device-end because the subagent might have to poll different modules to obtain data that are linked to different index entries. The recommended method is to ensure that a request has only objects that are linked to one index entry instead of multiple objects linked to different index entries.



NOTE: If responses from a device are slow, avoid using the **GetBulk** option for the device, because a **GetBulk** request might contain objects that are linked to various index entries and might further increase the response time.

Increasing Timeout Values in Polling and Discovery Intervals

By increasing the timeout values for polling and discovery intervals, you can increase the queuing time at the device end and reduce the number of throttle drops that occur because of the request timing out.

Reducing Incoming Packet Rate at the snmpd

By reducing the frequency of sending SNMP requests to a device, you can reduce the risk of SNMP requests piling up at any particular device. Apart from reducing the frequency of sending SNMP requests to a device, you can also increase the polling interval, control the use of **GetNext** requests, and reduce the number of polling stations per device.

Related Documentation

- [Understanding SNMP Implementation in Junos OS on page 1403](#)
- [Configuring SNMP on Devices Running Junos OS on page 1471](#)
- [Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS on page 1579](#)
- [Configuring Options on Managed Devices for Better SNMP Response Time on page 1469](#)
- *Managing Traps and Informs*
- *Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage*

Configuring Options on Managed Devices for Better SNMP Response Time

The following sections contain information about configuration options on the managed devices that can enhance SNMP performance:

- [Enabling the stats-cache-lifetime Option on page 1469](#)
- [Filtering Out Duplicate SNMP Requests on page 1469](#)
- [Excluding Interfaces That Are Slow in Responding to SNMP Queries on page 1470](#)

Enabling the stats-cache-lifetime Option

The Junos OS provides you with an option to configure the length of time an SNMP request stays active and queued so as to reduce the possibility of request drops during slow response times. You can use the **stats-cache-lifetime seconds** option at the **[edit snmp]** hierarchy level to specify the length of time that an SNMP request remains queued. The recommended value for the **stats-cache-lifetime** option is in the range of 30 to 60 seconds.



NOTE: The **set snmp stats-cache-lifetime seconds** command is a hidden command and is supported only on devices running Junos OS Release 9.3 and later.

Filtering Out Duplicate SNMP Requests

If a network management station retransmits a **Get**, **GetNext**, or **GetBulk** SNMP request too frequently to a device, that request might interfere with the processing of previous requests and slow down the response time of the agent. Filtering these duplicate requests improves the response time of the SNMP agent. The Junos OS enables you to filter out duplicate **Get**, **GetNext**, and **GetBulk** SNMP requests. The Junos OS uses the following information to determine if an SNMP request is a duplicate:

- Source IP address of the SNMP request
- Source UDP port of the SNMP request
- Request ID of the SNMP request



NOTE: By default, filtering of duplicate SNMP requests is disabled on devices running the Junos OS.

To enable filtering of duplicate SNMP requests on devices running the Junos OS, include the **filter-duplicates** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
filter-duplicates;
```

Excluding Interfaces That Are Slow in Responding to SNMP Queries

An interface that is slow in responding to SNMP requests for interface statistics can delay kernel responses to SNMP requests. You can review the mib2d log file to find out how long the kernel takes to respond to various SNMP requests. For more information about reviewing the log file for kernel response data, see “Checking Kernel and Packet Forwarding Engine Response” under “[Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS](#)” on page 1579. If you notice that a particular interface is slow in responding, and think that it is slowing down the kernel from responding to SNMP requests, exclude that interface from the SNMP queries to the device. You can exclude an interface from the SNMP queries either by configuring the **filter-interface** statement or by modifying the SNMP view settings.

The following example shows a sample configuration for excluding interfaces from the SNMP **Get**, **GetNext**, and **Set** operations:

```
[edit]
snmp {
  filter-interfaces {
    interfaces { # exclude the specified interfaces
      interface1;
      interface2;
    }
    all-internal-interfaces; # exclude all internal interfaces
  }
}
```

The following example shows the SNMP view configuration for excluding the interface with an interface index (ifIndex) value of 312 from a request for information related to the ifTable and ifXtable objects:

```
[edit snmp]
view test {
  oid .1 include;
  oid ifTable.1.*.312 exclude;
  oid ifXTable.1.*.312 exclude
}
```

Alternatively, you can take the interface that is slow in responding offline.

Related Documentation

- [Understanding SNMP Implementation in Junos OS on page 1403](#)
- [Configuring SNMP on Devices Running Junos OS on page 1471](#)
- [Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS on page 1579](#)
- [Optimizing the Network Management System Configuration for the Best Results on page 1467](#)
- *Managing Traps and Informs*
- *Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage*

Configuring SNMP on Devices Running Junos OS

The following sections contain information about basic SNMP configuration and a few examples of configuring the basic SNMP operations on devices running Junos OS:

- [Configuring Basic Settings for SNMPv1 and SNMPv2 on page 1471](#)
- [Configuring Basic Settings for SNMPv3 on page 1471](#)
- [Configuring System Name, Location, Description, and Contact Information on page 1473](#)

Configuring Basic Settings for SNMPv1 and SNMPv2

By default, SNMP is not enabled on devices running Junos OS. To enable SNMP on devices running Junos OS, include the **community public** statement at the **[edit snmp]** hierarchy level.

Enabling SNMPv1 and
SNMPv2 Get and
GetNext Operations

```
[edit]
snmp {
  community public;
}
```

A community that is defined as public grants access to all MIB data to any client.

To enable SNMPv1 and SNMPv2 **Set** operations on the device, you must include the following statements at the **[edit snmp]** hierarchy level:

Enabling SNMPv1 and
SNMPv2 Set
Operations

```
[edit snmp]
view all {
  oid .1;
}
community private {
  view all;
  authorization read-write;
}
```

The following example shows the basic minimum configuration for SNMPv1 and SNMPv2 traps on a device:

Configuring SNMPv1
and SNMPv2 Traps

```
[edit snmp]
trap-group jnpr {
  targets {
    192.168.69.179;
  }
}
```

Configuring Basic Settings for SNMPv3

The following example shows the minimum SNMPv3 configuration for enabling **Get**, **GetNext**, and **Set** operations on a device (note that the configuration has authentication set to **md5** and privacy to **none**):

Enabling SNMPv3 Get,
GetNext, and Set
Operations

```
[edit snmp]
v3 {
  usm {
    local-engine {
```

```

        user jnpruser {
            authentication-md5 {
                authentication-key "$9$guaDiQFnAuOQzevMWx7ikqP"; ## SECRET-DATA
            }
            privacy-none;
        }
    }
}
vacm {
    security-to-group {
        security-model usm {
            security-name jnpruser {
                group grpnm;
            }
        }
    }
}
access {
    group grpnm {
        default-context-prefix {
            security-model any {
                security-level authentication {
                    read-view all;
                    write-view all;
                }
            }
        }
    }
}
}
}
}
}
view all {
    oid .1;
}
}

```

The following example shows the basic configuration for SNMPv3 informs on a device (the configuration has authentication and privacy set to **none**):

Configuring SNMPv3 Informs	<pre> [edit snmp] v3 { usm { remote-engine 00000063000100a2c0a845b3 { user RU2_v3_sha_none { authentication-none; privacy-none; } } } } vacm { security-to-group { security-model usm { security-name RU2_v3_sha_none { group gl_usm_auth; } } } } access { </pre>
---------------------------------------	--


```

group g1_usm_auth {
  default-context-prefix {
    security-model usm {
      security-level authentication {
        read-view all;
        write-view all;
        notify-view all;
      }
    }
  }
}

target-address TA2_v3_sha_none {
  address 192.168.69.179;
  tag-list tl1;
  address-mask 255.255.252.0;
  target-parameters TP2_v3_sha_none;
}

target-parameters TP2_v3_sha_none {
  parameters {
    message-processing-model v3;
    security-model usm;
    security-level none;
    security-name RU2_v3_sha_none;
  }
  notify-filter nf1;
}

notify N1_all_tl1_informs {
  type inform; # Replace inform with trap to convert informs to traps.
  tag tl1;
}

notify-filter nf1 {
  oid .1 include;
}

view all {
  oid .1 include;
}

```

You can convert the SNMPv3 informs to traps by setting the value of the **type** statement at the **[edit snmp v3 notify N1_all_tl1_informs]** hierarchy level to **trap** as shown in the following example:

Converting Informs to Traps

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

Configuring System Name, Location, Description, and Contact Information

Junos OS enables you to include the name and location of the system, administrative contact information, and a brief description of the system in the SNMP configuration.



NOTE: Always keep the name, location, contact, and description information configured and updated for all your devices that are managed by SNMP.

The following example shows a typical configuration.



TIP: Use quotation marks to enclose the system name, contact, location, and description information that contain spaces.

```
[edit]
snmp {
  name "snmp 001"; # Overrides the system name.
  contact "Juniper Berry, (650) 555 1234"; # Specifies the name and phone number of
    the administrator.
  location "row 11, rack C"; # Specifies the location of the device.
  description "M40 router with 8 FPCs" # Configures a description for the device.
}
```

Related Documentation

- [FAQ: SNMP Support on Junos OS](#)
- [Understanding SNMP Implementation in Junos OS on page 1403](#)
- [Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS on page 1579](#)
- [Optimizing the Network Management System Configuration for the Best Results on page 1467](#)
- [Configuring Options on Managed Devices for Better SNMP Response Time on page 1469](#)
- [Managing Traps and Informs](#)
- [Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage](#)

Configuring the System Contact on a Device Running Junos OS

You can specify an administrative contact for each system being managed by SNMP. This name is placed into the MIB II **sysContact** object. To configure a contact name, include the **contact** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
contact contact;
```

If the name contains spaces, enclose it in quotation marks (" ").

To define a system contact name that contains spaces:

```
[edit]
snmp {
  contact "Juniper Berry, (650) 555-1234";
}
```

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuring the System Location for a Device Running Junos OS on page 1475](#)
- [Configuring the System Description on a Device Running Junos OS on page 1475](#)
- [Configuring a Different System Name on page 1477](#)

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring the System Location for a Device Running Junos OS

You can specify the location of each system being managed by SNMP. This string is placed into the MIB II **sysLocation** object. To configure a system location, include the **location** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
location location;
```

If the location contains spaces, enclose it in quotation marks (" ").

To specify the system location:

```
[edit]
snmp {
  location "Row 11, Rack C";
}
```

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1474](#)
- [Configuring the System Description on a Device Running Junos OS on page 1475](#)
- [Configuring a Different System Name on page 1477](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring the System Description on a Device Running Junos OS

You can specify a description for each system being managed by SNMP. This string is placed into the MIB II **sysDescription** object. To configure a description, include the **description** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
description description;
```

If the description contains spaces, enclose it in quotation marks (" ").

To specify the system description:

```
[edit]
snmp {
  description "M40 router with 8 FPCs";
}
```

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1474](#)
- [Configuring the System Location for a Device Running Junos OS on page 1475](#)
- [Configuring a Different System Name on page 1477](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring SNMP Details

You can use SNMP to store basic administrative details, such as a contact name and the location of the device. Your management system can then retrieve this information remotely, when you are troubleshooting an issue or performing an audit. In SNMP terminology, these are the `sysContact`, `sysDescription`, and `sysLocation` objects found within the system group of MIB-2 (as defined in RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*). You can set initial values directly in the Junos OS configuration for each system being managed by SNMP.

To set the system contact details:

1. Set the system contact details by including the **contact** statement at the **[edit snmp]** hierarchy level, or in an appropriate configuration group as shown here.

This administrative contact is placed into the MIB II **sysContact** object.

If the name contains spaces, enclose it in quotation marks (" ").

```
[edit groups global snmp]
user@host# set contact contact
```

For example:

```
[edit groups global snmp]
user@host# set contact "Enterprise Support, (650) 555-1234"
```

2. Configure a system description.

This string is placed into the MIB II **sysDescription** object. If the description contains spaces, enclose it in quotation marks (" ").

```
[edit groups global snmp]
user@host# set description description
```

For example:

```
[edit groups global snmp]
user@host# set description "M10i router with 8 FPCs"
```

3. Configure a system location.

This string is placed into the MIB II **sysLocation** object. If the location contains spaces, enclose it in quotation marks (" ").

To specify the system location:

```
[edit]
snmp {
  location "Row 11, Rack C";
}

[edit groups global snmp]
user@host# set location location
```

For example:

```
[edit groups global snmp]
user@host# set location "London Corporate Office, Lab 5, Row 11, Rack C"
```

4. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

5. Commit the configuration.

```
user@host# commit
```

6. To verify the configuration, enter the **show snmp mib walk system** operational-mode command.

The **show snmp mib walk system** command performs a MIB walk through of the system table (from MIB-2 as defined in RFC 1213). The SNMP agent in Junos OS responds by printing each row in the table and its associated value. You can use the same command to perform a MIB walk through any part of the MIB tree supported by the agent.

```
user@host> show snmp mib walk system
sysDescr.0    = M10i router with 8 FPCs
sysObjectID.0 = jnxProductNameM10i
sysUpTime.0   = 173676474
sysContact.0  = Enterprise Support, (650) 555-1234
sysName.0     = host
sysLocation.0 = London Corporate Office, Lab 5, Row 11, Rack C
sysServices.0 = 4
```

Related Documentation

- [Configuring SNMP Communities on page 1479](#)
- [Configuring SNMP Traps on page 1485](#)
- [Configuring SNMP on a Device Running Junos OS](#)

Configuring a Different System Name

Junos OS enables you to override the system name by including the **name** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
name name;
```

If the name contains spaces, enclose it in quotation marks (" ").

To specify the system name override:

```
[edit]
snmp {
  name "snmp1";
}
```

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1474](#)
- [Configuring the System Location for a Device Running Junos OS on page 1475](#)
- [Configuring the System Description on a Device Running Junos OS on page 1475](#)

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring the Commit Delay Timer

When a router or switch first receives an SNMP nonvolatile **Set** request, a Junos OS XML protocol session opens and prevents other users or applications from changing the candidate configuration (equivalent to the command-line interface [CLI] **configure exclusive** command). If the router does not receive new SNMP **Set** requests within 5 seconds (the default value), the candidate configuration is committed and the Junos OS XML protocol session closes (the configuration lock is released). If the router receives new SNMP **Set** requests while the candidate configuration is being committed, the SNMP **Set** request is rejected and an error is generated. If the router receives new SNMP **Set** requests before 5 seconds have elapsed, the commit-delay timer (the length of time between when the last SNMP request is received and the commit is requested) resets to 5 seconds.

By default, the timer is set to 5 seconds. To configure the timer for the SNMP **Set** reply and start of the commit, include the **commit-delay** statement at the **[edit snmp nonvolatile]** hierarchy level:

```
[edit snmp nonvolatile]
  commit-delay seconds;
```

seconds is the length of the time between when the SNMP request is received and the commit is requested for the candidate configuration. For more information about the **configure exclusive** command and locking the configuration, see the *CLI User Guide*.

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Filtering Duplicate SNMP Requests

By default, filtering duplicate **get**, **getNext**, and **getBulk** SNMP requests is disabled on devices running Junos OS. If a network management station retransmits a **Get**, **GetNext**, or **GetBulk** SNMP request too frequently to the router, that request might interfere with the processing of previous requests and slow down the response time of the agent. Filtering these duplicate requests improves the response time of the SNMP agent. Junos OS uses the following information to determine if an SNMP request is a duplicate:

- Source IP address of the SNMP request
- Source UDP port of the SNMP request
- Request ID of the SNMP request

To filter duplicate SNMP requests, include the **filter-duplicates** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
  filter-duplicates;
```

- Related Documentation**
- [Configuring SNMP on a Device Running Junos OS](#)
 - [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1494](#)
 - [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1495](#)
 - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring SNMP Communities

Configuring the SNMP agent in Junos OS is a straightforward task that shares many familiar settings common to other managed devices in your network. For example, you need to configure Junos OS with an SNMP community string and a destination for traps. Community strings are administrative names that group collections of devices and the agents that are running on them together into common management domains. If a manager and an agent share the same community, they can communicate with each other. An SNMP community defines the level of authorization granted to its members, such as which MIB objects are available, which operations (read-only or read-write) are valid for those objects, and which SNMP clients are authorized, based on their source IP addresses.

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server.

To create a read-only SNMP community:

1. Enter the SNMP community used in your network.

If the community name contains spaces, enclose it in quotation marks (" ").

Community names must be unique.



NOTE: You cannot configure the same community name at the [edit snmp community] and [edit snmp v3 snmp-community *community-index*] hierarchy levels.

```
[edit groups global]
user@host# set snmp community name
```

This example uses the standard name **public** to create a community that gives limited read-only access.

```
[edit groups global]
user@host# set snmp community public
```

2. Define the authorization level for the community.

The default authorization level for a community is **read-only**.

To allow **Set** requests within a community, you need to define that community as **authorization read-write**. For **Set** requests, you also need to include the specific MIB objects that are accessible with read-write privileges using the **view** statement. The

default view includes all supported MIB objects that are accessible with read-only privileges. No MIB objects are accessible with read-write privileges. For more information about the **view** statement, see [“Configuring MIB Views” on page 1496](#).

```
[edit groups global snmp community name]  
user@host# set authorization authorization
```

This example confines the public community to read-only access. Any SNMP client (for example, an SNMP management system) that belongs to the public community can read MIB variables but cannot set (change) them.

```
[edit groups global snmp community public]  
user@host# set authorization read-only
```

3. Define a list of clients in the community who are authorized to communicate with the SNMP agent in Junos OS.

The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. List the clients by IP address and prefix. Typically, the list includes the SNMP network management system in your network or the address of your management network. If no **clients** statement is present, all clients are allowed. For **address**, you must specify an IPv4 or IPv6 address, not a hostname.

```
[edit groups global snmp community name]  
user@host# set clients address
```

The following statement defines the hosts in the 192.168.1.0/24 network as being authorized in the public community.

```
[edit groups global snmp community public]  
user@host# set clients 192.168.1.0/24
```

4. Define the clients that are not authorized within the community by specifying their IP address, followed by the **restrict** statement.

```
[edit groups global snmp community name]  
user@host# set clients address restrict
```

The following statement defines all other hosts as being restricted from the public community.

```
[edit groups global snmp community public]  
user@host# set clients 0/0 restrict
```

5. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]  
user@host# set apply-groups global
```

6. Commit the configuration.

```
user@host# commit
```

To create a read-write SNMP community:

1. Enter the SNMP community used in your network.

```
[edit groups global]  
user@host# set snmp community name
```


This example standard community string **private** to identify the community granted read-write access to the SNMP agent running on the device.

```
[edit groups global]
user@host# set snmp community private
```

2. Define the authorization level for the community.

```
[edit groups global snmp community name]
user@host# set authorization authorization
```

This example confines the public community to read-only access. Any SNMP client (for example, an SNMP management system) that belongs to the public community can read MIB variables but cannot set (change) them.

```
[edit groups global snmp community public]
user@host# set authorization read-write
```

3. Define a list of clients in the community who are authorized to make changes to the SNMP agent in Junos OS.

List the clients by IP address and prefix.

```
[edit groups global snmp community name]
user@host# set clients address
```

For example:

```
[edit groups global snmp community private]
user@host# set clients 192.168.1.15/24
user@host# set clients 192.168.1.18/24
```

4. Define the clients that are not authorized within the community by specifying their IP address, followed by the **restrict** statement.

```
[edit groups global snmp community name]
user@host# set clients address restrict
```

The following statement defines all other hosts as being restricted from the public community.

```
[edit groups global snmp community private]
user@host# set clients 0/0 restrict
```

5. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

6. Commit the configuration.

```
user@host# commit
```

Related Documentation

- [Adding a Group of Clients to an SNMP Community on page 1482](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
- [Examples: Configuring the SNMP Community String on page 1482](#)

Examples: Configuring the SNMP Community String

Grant read-only access to all clients. With the following configuration, the system responds to SNMP **Get**, **GetNext**, and **GetBulk** requests that contain the community string **public**:

```
[edit]
snmp {
  community public {
    authorization read-only;
  }
}
```

Grant all clients read-write access to the ping MIB and **jnxPingMIB**. With the following configuration, the system responds to SNMP **Get**, **GetNext**, **GetBulk**, and **Set** requests that contain the community string **private** and specify an OID contained in the ping MIB or **jnxPingMIB** hierarchy:

```
[edit]
snmp {
  view ping-mib-view {
    oid pingMIB include;
    oid jnxPingMIB include;
    community private {
      authorization read-write;
      view ping-mib-view;
    }
  }
}
```

The following configuration allows read-only access to clients with IP addresses in the range **1.2.3.4/24**, and denies access to systems in the range **fe80::1:2:3:4/64**:

```
[edit]
snmp {
  community field-service {
    authorization read-only;
    clients {
      default restrict; # Restrict access to all SNMP clients not explicitly
                        # listed on the following lines.
      1.2.3.4/24; # Allow access by all clients in 1.2.3.4/24 except
      fe80::1:2:3:4/64 restrict; # fe80::1:2:3:4/64.
    }
  }
}
```

Related Documentation

- [Configuring SNMP Communities on page 1479](#)

Adding a Group of Clients to an SNMP Community

Junos OS enables you to add one or more groups of clients to an SNMP community. You can include the **client-list-name** *name* statement at the **[edit snmp community community-name]** hierarchy level to add all the members of the client list or prefix list to an SNMP community.

To define a list of clients, include the **client-list** statement followed by the IP addresses of the clients at the **[edit snmp]** hierarchy level:

```
[edit snmp]
  client-list client-list-name {
    ip-addresses;
  }
```

You can configure a prefix list at the **[edit policy options]** hierarchy level. Support for prefix lists in the SNMP community configuration enables you to use a single list to configure the SNMP and routing policies. For more information about the **prefix-list** statement, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

To add a client list or prefix list to an SNMP community, include the **client-list-name** statement at the **[edit snmp community community-name]** hierarchy level:

```
[edit snmp community community-name]
  client-list-name client-list-name;
```



NOTE: The client list and prefix list must not have the same name.

The following example shows how to define a client list:

```
[edit]
snmp {
  client-list clentlist1 {
    10.1.1.1/32;
    10.2.2.2/32;
  }
}
```

The following example shows how to add a client list to an SNMP community:

```
[edit]
snmp {
  community community1 {
    authorization read-only;
    client-list-name clientlist1;
  }
}
```

The following example shows how to add a prefix list to an SNMP community:

```
[edit]
policy-options {
  prefix-list prefixlist {
    10.3.3.3/32;
    10.5.5.5/32;
  }
}
snmp {
  community community2 {
    client-list-name prefixlist;
  }
}
```

- Related Documentation**
- *client-list*
 - *client-list-name*

Configuring a Proxy SNMP Agent

Junos OS enables you to assign one of the devices in the network as a proxy SNMP agent through which the network management system (NMS) can query other devices in the network. When you configure a proxy, you can specify the names of devices to be managed through the proxy SNMP agent.

When the NMS queries the proxy SNMP agent, the NMS specifies the community name (for SNMPv1 and SNMPv2) or the context and security name (for SNMPv3) associated with the device from which it requires the information.



NOTE: If you have configured authentication and privacy methods and passwords for SNMPv3, those parameters are also specified in the query for SNMPv3 information.

To configure a proxy SNMP agent and specify devices to be managed by the proxy SNMP agent, you can include the following configuration statements at the `[edit snmp]` hierarchy level:

```
proxy proxy-name{
  device-name device-name;
  logical-system logical-system {
    routing-instance routing-instance;
  }
  routing-instance routing-instance;
  <version-v1 | version-v2c> {
    snmp-community community-name;
    no-default-comm-to-v3-config;
  }
  version-v3 {
    security-name security-name;
    context context-name;
  }
}
```

- The **proxy** statement enables you to specify a unique name for the proxy configuration.
- The **version-v1**, **version-v2c**, and **version-v3** statements enable you to specify the SNMP version.
- The **no-default-comm-to-v3-config** statement is an optional statement at the `[edit snmp proxy proxy-name <version-v1 | version-v2c>]` hierarchy level that when included in the configuration requires you to manually configure the statements at the `[edit snmp v3 snmp-community community-name]` and `[edit snmp v3 vacm]` hierarchy levels.

If the **no-default-comm-to-v3-config** statement is not included at the `[edit snmp proxy proxy-name <version-v1 | version-v2c>]` hierarchy level, the `[edit snmp v3`

`snmp-community community-name`] and `[edit snmp v3 vacm]` hierarchy level configurations are automatically initialized.

- The **logical-system** and **routing-instance** statements are optional statements that enable you to specify logical system and routing instance names if you want to create proxies for logical systems or routing instances on the device.



NOTE: The community and security configuration for the proxy should match the corresponding configuration on the device that is to be managed.



NOTE: Because the proxy SNMP agent does not have trap forwarding capabilities, the devices that are managed by the proxy SNMP agent send the traps directly to the network management system.

You can use the **show snmp proxy** operational mode command to view proxy details on a device. The **show snmp proxy** command returns the proxy names, device names, SNMP version, community/security, and context information.

Related Documentation

- [proxy \(snmp\) on page 2061](#)

Configuring SNMP Traps

Traps are unsolicited messages sent from an SNMP agent to remote network management systems or trap receivers. Many enterprises use SNMP traps as part of a fault-monitoring solution, in addition to system logging. In Junos OS, SNMP traps are not forwarded by default, so you must configure a trap-group if you wish to use SNMP traps.

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name.

To configure an SNMP trap:

1. Create a single, consistent source address that Junos OS applies to all outgoing traps in your device.

A source address is useful, because although most Junos OS devices have a number of outbound interfaces, using one source address helps a remote NMS to associate the source of the traps with an individual device

```
[edit groups global snmp]
user@host# set trap-options source-address address
```

This example uses the IP address of the loopback interface (lo0) as the source address for all the SNMP traps that originate from the device.

```
[edit groups global snmp]
user@host# set trap-options source-address lo0
```

2. Create a trap group in which you can list the types of traps to be forwarded and the targets (addresses) of the receiving remote management systems.

```
[edit groups global snmp trap-group group-name]
user@host# set version (all | v1 | v2) targets address
```

This example creates a trap group called **managers**, allows SNMP version 2-formatted notifications (traps) to be sent to the host at address 192.168.1.15. This statement forwards all categories of traps.

```
[edit groups global snmp trap-group managers]
user@host# set version v2 targets 192.168.1.15
```

3. Define the specific subset of trap categories to be forwarded.

For a list of categories, see [“Configuring SNMP Trap Groups” on page 1491](#).

```
[edit groups global snmp trap-group group-name]
user@host# set categories category
```

The following statement configures the standard MIB-II authentication failures on the agent (the device).

```
[edit groups global snmp trap-group managers]
user@host# set categories authentication
```

4. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

5. Commit the configuration.

```
user@host# commit
```

6. To verify the configuration, generate an authentication failure trap.

This means that the SNMP agent received a request with an unknown community. Other traps types can also be spoofed as well.

This feature enables you to trigger SNMP traps from routers and ensure that they are processed correctly within your existing network management infrastructure. This is also useful for testing and debugging SNMP behavior on the switch or NMS.

Using the **monitor traffic** command, you can verify that the trap is sent to the network management system.

```
user@host> request snmp spoof-trap spoof-trap authenticationFailure
Spoof-trap request result: trap sent successfully
```

Related Documentation

- [Adding a Group of Clients to an SNMP Community on page 1482](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
- [Examples: Configuring the SNMP Community String on page 1482](#)

Configuring SNMP Trap Options and Groups on a Device Running Junos OS

Some carriers have more than one trap receiver that forwards traps to a central NMS. This allows for more than one path for SNMP traps from a router to the central NMS through different trap receivers. A device running Junos OS can be configured to send the same copy of each SNMP trap to every trap receiver configured in the trap group.

The source address in the IP header of each SNMP trap packet is set to the address of the outgoing interface by default. When a trap receiver forwards the packet to the central NMS, the source address is preserved. The central NMS, looking only at the source address of each SNMP trap packet, assumes that each SNMP trap came from a different source.

In reality, the SNMP traps came from the same router, but each left the router through a different outgoing interface.

The statements discussed in the following sections are provided to allow the NMS to recognize the duplicate traps and to distinguish SNMPv1 traps based on the outgoing interface.

To configure SNMP trap options and trap groups, include the **trap-options** and **trap-group** statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-options {
  agent-address outgoing-interface;
  source-address address;
}
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

Related Documentation

- [Configuring SNMP Trap Options on page 1487](#)
- [Configuring SNMP Trap Groups on page 1491](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring SNMP Trap Options

Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router to a single address regardless of the outgoing interface. In addition, you can set the agent address of the SNMPv1 traps. For more information about the contents of SNMPv1 traps, see RFC 1157.



NOTE: SNMP cannot be associated with any routing instances other than the master routing instance.

To configure SNMP trap options, include the **trap-options** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-options {
  agent-address outgoing-interface;
  enterprise-oid
  logical-system
  routing-instance
  source-address address;
}
```

You must also configure a trap group for the trap options to take effect. For information about trap groups, see “Configuring SNMP Trap Groups” on page 1491.

This topic contains the following sections:

- [Configuring the Source Address for SNMP Traps on page 1488](#)
- [Configuring the Agent Address for SNMP Traps on page 1490](#)
- [Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps on page 1491](#)

Configuring the Source Address for SNMP Traps

You can configure the source address of trap packets in many ways: **lo0**, a valid IPv4 address or IPv6 address configured on one of the router interfaces, a logical-system address, or the address of a routing-instance. The value **lo0** indicates that the source address of the SNMP trap packets is set to the lowest loopback address configured on the interface **lo0**.



NOTE: If the source address is an invalid IPv4 or IPv6 address or is not configured, SNMP traps are not generated.

You can configure the source address of trap packets in one of the following formats:

- A valid IPv4 address configured on one of the router interfaces
- A valid IPv6 address configured on one of the router interfaces
- **lo0**; that is, the lowest loopback address configured on the interface **lo0**
- A logical-system name
- A routing-instance name

A Valid IPv4 Address As the Source Address

To specify a valid IPv4 interface address as the source address for SNMP traps on one of the router interfaces, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
```



```
source-address address;
```

address is a valid IPv4 address configured on one of the router interfaces.

A Valid IPv6 Address As the Source Address

To specify a valid IPv6 interface address as the source address for SNMP traps on one of the router interfaces, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
source-address address;
```

address is a valid IPv6 address configured on one of the router interfaces.

The Lowest Loopback Address As the Source Address

To specify the source address of the SNMP traps so that they use the lowest loopback address configured on the interface **lo0** as the source address, include the **source-address** statement at the **[edit snmp trap-options]** hierarchy level:

```
[edit snmp trap-options]
source-address lo0;
```

To enable and configure the loopback address, include the **address** statement at the **[edit interfaces lo0 unit 0 family inet]** hierarchy level:

```
[edit interfaces]
lo0 {
  unit 0 {
    family inet {
      address ip-address;
    }
  }
}
```

To configure the loopback address as the source address of trap packets:

```
[edit snmp]
trap-options {
  source-address lo0;
}
trap-group "urgent-dispatcher" {
  version v2;
  categories link startup;
  targets {
    192.168.10.22;
    172.17.1.2;
  }
}
[edit interfaces]
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.1/32;
      address 127.0.0.1/32;
    }
  }
}
```

In this example, the IP address **10.0.0.1** is the source address of every trap sent from this router.

Logical System Name as the Source Address To specify a logical system name as the source address of SNMP traps, include the **logical-system** *logical-system-name* statement at the **[edit snmp trap-options]** hierarchy level.

For example, the following configuration sets logical system name **ls1** as the source address of SNMP traps:

```
[edit snmp]
  trap-options {
    logical-system ls1;
  }
```

Routing Instance Name as the Source Address To specify a routing instance name as the source address of SNMP traps, include the **routing-instance** *routing-instance-name* statement at the **[edit snmp trap-options]** hierarchy level.

For example, the following configuration sets the routing instance name **ri1** as the source address for SNMP traps:

```
[edit snmp]
  trap-options {
    routing-instance ri1;
  }
```

Configuring the Agent Address for SNMP Traps

The agent address is only available in SNMPv1 trap packets (see RFC 1157). By default, the router's default local address is not specified in the agent address field of the SNMPv1 trap. To configure the agent address, include the **agent-address** statement at the **[edit snmp trap-options]** hierarchy level. Currently, the agent address can only be the address of the outgoing interface:

```
[edit snmp]
  trap-options {
    agent-address outgoing-interface;
  }
```

To configure the outgoing interface as the agent address:

```
[edit snmp]
  trap-options {
    agent-address outgoing-interface;
  }
  trap-group "urgent-dispatcher" {
    version v1;
    categories link startup;
    targets {
      192.168.10.22;
      172.17.1.2;
    }
  }
```

In this example, each SNMPv1 trap packet sent has its agent address value set to the IP address of the outgoing interface.

Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps

The **snmpTrapEnterprise** object helps you identify the enterprise that has defined the trap. Typically, the **snmpTrapEnterprise** object appears as the last varbind in enterprise-specific SNMP version 2 traps. However, starting Release 10.0, Junos OS enables you to add the **snmpTrapEnterprise** object identifier to standard SNMP traps as well.

To add **snmpTrapEnterprise** to standard traps, include the **enterprise-oid** statement at the **[edit snmp trap-options]** hierarchy level. If the **enterprise-oid** statement is not included in the configuration, **snmpTrapEnterprise** is added only for enterprise-specific traps.

```
[edit snmp]
trap-options {
  enterprise-oid;
}
```

Related Documentation

- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
- [Configuring SNMP Trap Groups on page 1491](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring SNMP Trap Groups

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. The trap group must be configured for SNMP traps to be sent. To create an SNMP trap group, include the **trap-group** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  routing-instance instance;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, include the **destination-port** statement. The default destination port is port 162.

For each trap group that you define, you must include the **target** statement to define at least one system as the recipient of the SNMP traps in the trap group. Specify the IPv4 or IPv6 address of each recipient, not its hostname.

Specify the types of traps the trap group can receive in the **categories** statement. For information about the category to which the traps belong, see the [“Standard SNMP Traps Supported on Devices Running Junos OS” on page 1456](#) and [“Juniper Networks Enterprise-Specific SNMP Traps” on page 1456](#) topics.

Specify the routing instance used by the trap group in the **routing-instance** statement. All targets configured in the trap group use this routing instance.

A trap group can receive the following categories:

- **authentication**—Authentication failures
- **chassis**—Chassis or environment notifications
- **configuration**—Configuration notifications
- **link**—Link-related notifications (up-down transitions, DS-3 and DS-1 line status change, IPv6 interface state change, and Passive Monitoring PIC overload)



NOTE: To send Passive Monitoring PIC overload interface traps, select the **link** trap category.

- **remote-operations**—Remote operation notifications
- **rmon-alarm**—Alarm for RMON events
- **routing**—Routing protocol notifications
- **sonet-alarms**—SONET/SDH alarms



NOTE: If you omit the SONET/SDH subcategories, all SONET/SDH trap alarm types are included in trap notifications.

- **loss-of-light**—Loss of light alarm notification
- **pll-lock**—PLL lock alarm notification
- **loss-of-frame**—Loss of frame alarm notification
- **loss-of-signal**—Loss of signal alarm notification
- **severely-errored-frame**—Severely errored frame alarm notification
- **line-ais**—Line alarm indication signal (AIS) alarm notification
- **path-ais**—Path AIS alarm notification
- **loss-of-pointer**—Loss of pointer alarm notification
- **ber-defect**—SONET/SDH bit error rate alarm defect notification
- **ber-fault**—SONET/SDH error rate alarm fault notification
- **line-remote-defect-indication**—Line remote defect indication alarm notification
- **path-remote-defect-indication**—Path remote defect indication alarm notification

- **remote-error-indication**—Remote error indication alarm notification
- **unequipped**—Unequipped alarm notification
- **path-mismatch**—Path mismatch alarm notification
- **loss-of-cell**—Loss of cell delineation alarm notification
- **vt-ais**—Virtual tributary (VT) AIS alarm notification
- **vt-loss-of-pointer**—VT loss of pointer alarm notification
- **vt-remote-defect-indication**—VT remote defect indication alarm notification
- **vt-unequipped**—VT unequipped alarm notification
- **vt-label-mismatch**—VT label mismatch error notification
- **vt-loss-of-cell**—VT loss of cell delineation notification
- **startup**—System warm and cold starts
- **timing-events**—Timing events and defects notification
- **vrp-events**—Virtual Router Redundancy Protocol (VRRP) events such as new-master or authentication failures
- **startup**—System warm and cold starts
- **vrp-events**—Virtual Router Redundancy Protocol (VRRP) events such as new-master or authentication failures

If you include SONET/SDH subcategories, only those SONET/SDH trap alarm types are included in trap notifications.

The **version** statement allows you to specify the SNMP version of the traps sent to targets of the trap group. If you specify **v1** only, SNMPv1 traps are sent. If you specify **v2** only, SNMPv2 traps are sent. If you specify **all**, both an SNMPv1 and an SNMPv2 trap are sent for every trap condition. For more information about the **version** statement, see [version \(SNMP\)](#).

Related Documentation

- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
- [Configuring SNMP Trap Options on page 1487](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
- [Example: Configuring SNMP Trap Groups on page 1493](#)

Example: Configuring SNMP Trap Groups

Set up a trap notification list named **urgent-dispatcher** for link and startup traps. This list is used to identify the network management hosts (1.2.3.4 and fe80::1:2:3:4) to which traps generated by the local router should be sent. The name specified for a trap group is used as the SNMP community string when the agent sends traps to the listed targets.

[edit]

```
snmp {
  trap-group "urgent-dispatcher" {
    version v2;
    categories link startup;
    targets {
      1.2.3.4;
      fe80::1:2:3:4;
    }
  }
}
```

- Related Documentation**
- [Configuring SNMP Trap Groups on page 1491](#)
 - [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1487](#)
 - [Configuring SNMP Trap Options on page 1487](#)

Configuring the Interfaces on Which SNMP Requests Can Be Accepted

By default, all router or switch interfaces have SNMP access privileges. To limit the access through certain interfaces only, include the **interface** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
interface [ interface-names ];
```

Specify the names of any logical or physical interfaces that should have SNMP access privileges. Any SNMP requests entering the router or switch from interfaces not listed are discarded.

- Related Documentation**
- [Configuring SNMP on a Device Running Junos OS](#)
 - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
 - [Example: Configuring Secured Access List Checking on page 1494](#)

Example: Configuring Secured Access List Checking

SNMP access privileges are granted to only devices on interfaces **so-0/0/0** and **at-1/0/1**. The following example does this by configuring a list of logical interfaces:

```
[edit]
snmp {
  interface [ so-0/0/0.0 so-0/0/0.1 at-1/0/1.0 at-1/0/1.1 ];
}
```

The following example grants the same access by configuring a list of physical interfaces:

```
[edit]
snmp {
  interface [ so-0/0/0 at-1/0/1 ];
}
```

- Related Documentation**
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1494](#)

- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1495](#)
- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Filtering Interface Information Out of SNMP Get and GetNext Output

Junos OS enables you to filter out information related to specific interfaces from the output of SNMP **Get** and **GetNext** requests performed on interface-related MIBs such as IF MIB, ATM MIB, RMON MIB, and the Juniper Networks enterprise-specific IF MIB.

You can use the following options of the **filter-interfaces** statement at the **[edit snmp]** hierarchy level to specify the interfaces that you want to exclude from SNMP **Get** and **GetNext** queries:

- **interfaces**—Interfaces that match the specified regular expressions.
- **all-internal-interfaces**—Internal interfaces.

```
[edit]
snmp {
  filter-interfaces {
    interfaces {
      interface-name 1;
      interface-name 2;
    }
    all-internal-interfaces;
  }
}
```

Starting with Release 12.1, Junos OS provides an except option (! operator) that enables you to filter out all interfaces except those interfaces that match all the regular expressions prefixed with the ! mark.

For example, to filter out all interfaces except the **ge** interfaces from the SNMP **get** and **get-next** results, enter the following command:

```
[edit snmp]
user@host# set filter-interfaces interfaces "!^~ge-.*"
user@host# commit
```

When this is configured, Junos OS filters out all interfaces except the **ge** interfaces from the SNMP **get** and **get-next** results.



NOTE: The ! mark is supported only as the first character of the regular expression. If it appears anywhere else in a regular expression, Junos OS considers the regular expression invalid, and returns an error.

However, note that these settings are limited to SNMP operations, and the users can continue to access information related to the interfaces (including those hidden using

the **filter-interfaces** options) using the appropriate Junos OS command-line interface (CLI) commands.

- Related Documentation**
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1494](#)
 - [Configuring SNMP on a Device Running Junos OS](#)
 - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

Configuring MIB Views

SNMPv3 defines the concept of MIB views in RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. MIB views provide an agent better control over who can access specific branches and objects within its MIB tree. A view consists of a name and a collection of SNMP object identifiers, which are either explicitly included or excluded. Once defined, a view is then assigned to an SNMPv3 group or SNMPv1/v2c community (or multiple communities), automatically masking which parts of the agent's MIB tree members of the group or community can (or cannot) access.

By default, an SNMP community grants read access and denies write access to all supported MIB objects (even communities configured as **authorization read-write**). To restrict or grant read or write access to a set of MIB objects, you must configure a MIB view and associate the view with a community.

To configure MIB views, include the **view** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
view view-name {
  oid object-identifier (include | exclude);
}
```

The **view** statement defines a MIB view and identifies a group of MIB objects. Each MIB object of a view has a common object identifier (OID) prefix. Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). A configuration statement uses a view to specify a group of MIB objects on which to define access. You can also use a wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, you must associate the view with a community.



NOTE: To remove an OID completely, use the **delete view all oid oid-number** command but omit the **include** parameter.

To associate MIB views with a community, include the **view** statement at the **[edit snmp community community-name]** hierarchy level:

```
[edit snmp community community-name]
view view-name;
```

For more information about the Ping MIB, see RFC 2925 and the *PING MIB* topic.

- Related Documentation**
- [PING MIB](#)
 - [Configuring SNMP on a Device Running Junos OS](#)
 - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
 - [Example: Ping Proxy MIB on page 1497](#)
 - [view \(Configuring a MIB View\) on page 2070](#)
 - [view \(Associating MIB View with a Community\)](#)
 - [oid on page 2060](#)

Example: Ping Proxy MIB

Restrict the **ping-mib** community to read and write access of the Ping MIB and **jnxpingMIB** only. Read or write access to any other MIB using this community is not allowed.

```
[edit snmp]
view ping-mib-view {
  oid 1.3.6.1.2.1.80 include; #pingMIB
  oid jnxPingMIB include; #jnxPingMIB
}
community ping-mib {
  authorization read-write;
  view ping-mib-view;
}
```

The following configuration prevents the **no-ping-mib** community from accessing Ping MIB and **jnxPingMIB** objects. However, this configuration does not prevent the **no-ping-mib** community from accessing any other MIB object that is supported on the device.

```
[edit snmp]
view no-ping-mib-view {
  oid 1.3.6.1.2.1.80 exclude; # deny access to pingMIB objects
  oid jnxPingMIB exclude; # deny access to jnxPingMIB objects
}
community no-ping-mib {
  authorization read-write;
  view ping-mib-view;
}
```

- Related Documentation**
- [Configuring SNMP on a Device Running Junos OS](#)
 - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
 - [Configuring MIB Views on page 1496](#)
 - [view \(Configuring a MIB View\) on page 2070](#)
 - [oid on page 2060](#)

CHAPTER 64

Configuring SNMPv3

- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: SNMPv3 Configuration on page 1503](#)
- [Configuring the Local Engine ID on page 1506](#)
- [Creating SNMPv3 Users on page 1507](#)
- [Example: Creating SNMPv3 Users on page 1508](#)
- [Configuring the SNMPv3 Authentication Type on page 1509](#)
- [Configuring the SNMPv3 Encryption Type on page 1510](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring the Access Privileges Granted to a Group on page 1513](#)
- [Example: Configuring the Access Privileges Granted to a Group on page 1516](#)
- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Example: Security Group Configuration on page 1519](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the SNMPv3 Trap Notification on page 1520](#)
- [Example: Configuring SNMPv3 Trap Notification on page 1521](#)
- [Configuring the Trap Notification Filter on page 1522](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Example: Configuring the Tag List on page 1525](#)
- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Configuring SNMP Informs on page 1529](#)
- [Configuring the Remote Engine and Remote User on page 1530](#)
- [Example: Configuring the Remote Engine ID and Remote User on page 1531](#)
- [Configuring the Inform Notification Type and Target Address on page 1534](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1536](#)
- [Configuring the SNMPv3 Community on page 1536](#)
- [Example: Configuring an SNMPv3 Community on page 1539](#)

Complete SNMPv3 Configuration Statements

To configure SNMPv3, include the following statements at the `[edit snmp v3]` and `[edit snmp]` hierarchy levels:

```
[edit snmp]
engine-id {
  (local engine-id | use-mac-address | use-default-ip-address);
}
view view-name {
  oid object-identifier (include | exclude);
}

[edit snmp v3]
notify name {
  tag tag-name;
  type (trap | inform);
}
notify-filter profile-name {
  oid object-identifier (include | exclude);
}
snmp-community community-index {
  community-name community-name;
  security-name security-name;
  tag tag-name;
}
target-address target-address-name {
  address address;
  address-mask address-mask;
  logical-system logical-system;
  port port-number;
  retry-count number;
  routing-instance instance;
  tag-list tag-list;
  target-parameters target-parameters-name;
  timeout seconds;
}
target-parameters target-parameters-name {
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
usm {
  (local-engine | remote-engine engine-id) {
    user username {
      authentication-md5 {
        authentication-password authentication-password;
      }
      authentication-none;
      authentication-sha {
        authentication-password authentication-password;
      }
    }
  }
}
```

```

    }
    privacy-3des {
        privacy-password privacy-password;
    }
    privacy-aes128 {
        privacy-password privacy-password;
    }
    privacy-des {
        privacy-password privacy-password;
    }
    privacy-none;
}
}
}
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix){
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
}
}

```

Related Documentation

- [Creating SNMPv3 Users on page 1507](#)
- [Configuring MIB Views on page 1496](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring SNMP Informs on page 1529](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Minimum SNMPv3 Configuration on a Device Running Junos OS

To configure the minimum requirements for SNMPv3, include the following statements at the `[edit snmp v3]` and `[edit snmp]` hierarchy levels:



NOTE: You must configure at least one view (notify, read, or write) at the `[edit snmp view-name]` hierarchy level.

```
[edit snmp]
view view-name {
  oid object-identifier (include | exclude);
}
[edit snmp v3]
notify name {
  tag tag-name;
}
notify-filter profile-name {
  oid object-identifier (include | exclude);
}
snmp-community community-index {
  security-name security-name;
}
target-address target-address-name {
  address address;
  target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
usm {
  local-engine {
    user username {
    }
  }
}
vacm {
  access {
    group group-name {
      (default-context-prefix | context-prefix context-prefix){
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
}
```

```

    }
  }
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}
}

```

**Related
Documentation**

- [Creating SNMPv3 Users on page 1507](#)
- [Configuring MIB Views on page 1496](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring SNMP Informs on page 1529](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Example: SNMPv3 Configuration on page 1503](#)

Example: SNMPv3 Configuration

Define an SNMPv3 configuration:

```

[edit snmp]
engine-id {
  use-mac-address;
}
view jnxAlarms {
  oid 1.3.6.1.4.1.2636.3.4 include;
}
view interfaces {
  oid 1.3.6.1.2.1.2 include;
}
view ping-mib {
  oid 1.3.6.1.2.1.80 include;
}
[edit snmp v3]
notify n1 {
  tag router1; # Identifies a set of target addresses
  type trap; # Defines type of notification
}
notify n2 {
  tag host1;
  type trap;
}
notify-filter nf1 {
  oid .1 include; # Defines which traps to send
} # In this case, includes all traps
notify-filter nf2 {

```

```

    oid 1.3.6.1.4.1 include; # Sends enterprise-specific traps only
  }
  notify-filter nf3 {
    oid 1.3.6.1.2.1.1.5 include; # Sends BGP traps only
  }
  snmp-community index1 {
    community-name "$9$JOZi.QF/AtOz3"; # SECRET-DATA
    security-name john; # Matches the security name at the target parameters
    tag host1; # Finds the addresses that are allowed to be used with
  }
  target-address ta1 { # Associates the target address with the group
    # san-francisco.
    address 10.1.1.1;
    address-mask 255.255.255.0; # Defines the range of addresses
    port 162;
    tag-list router1;
    target-parameters tp1; # Applies configured target parameters
  }
  target-address ta2 {
    address 10.1.1.2;
    address-mask 255.255.255.0;
    port 162;
    tag-list host1;
    target-parameters tp2;
  }
  target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list "router1 host1";
    target-parameters tp3;
  }
  target-parameters tp1 { # Defines the target parameters
    notify-filter nf1; # Specifies which notify filter to apply
    parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
      security-name john; # Matches the security name configured at the
    } # [edit snmp v3 snmp-community community-index hierarchy level.
  }
  target-parameters tp2 {
    notify-filter nf2;
    parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;
      security-name john;
    }
  }
  target-parameters tp3 {
    notify-filter nf3;
    parameters {
      message-processing-model v1;
      security-model v1;
      security-level none;

```



```

        security-name john;
    }
}
usm {
    local-engine { #Defines authentication and encryption for SNMPv3 users
        user user1 {
            authentication-md5 {
                authentication-password authentication-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
        }
        user user2 {
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
        user user3 {
            authentication-none;
            privacy-none;
        }
        user user4 {
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
        }
        user user5 {
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
    }
}
vacm {
    access {
        group san-francisco { #Defines the access privileges for the group
            default-context-prefix { # called san-francisco
                security-model v1 {
                    security-level none {
                        notify-view ping-mib;
                        read-view interfaces;
                        write-view jnxAlarms;
                    }
                }
            }
        }
    }
}
security-to-group {
    security-model v1 {
        security-name john { # Assigns john to the security group

```

```

        group san-francisco; # called san-francisco
    }
    security-name bob {
        group new-york;
    }
    security-name elizabeth {
        group chicago;
    }
}
}
}

```

- Related Documentation**
- [Complete SNMPv3 Configuration Statements on page 1500](#)
 - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the Local Engine ID

By default, the local engine ID uses the default IP address of the router. The local engine ID is the administratively unique identifier for the SNMPv3 engine. This statement is optional. To configure the local engine ID, include the **engine-id** statement at the **[edit snmp]** hierarchy level:

```

[edit snmp]
engine-id {
    (local engine-id-suffix | use-default-ip-address | use-mac-address);
}

```

- **local engine-id-suffix**—The engine ID suffix is explicitly configured.
- **use-default-ip-address**—The engine ID suffix is generated from the default IP address.
- **use-mac-address**—The SNMP engine identifier is generated from the Media Access Control (MAC) address of the management interface on the router.

The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*. You can configure the suffix here.



NOTE: SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords are based on the previous engine ID. For the engine ID, we recommend using the master IP address of the device if the device has multiple routing engines and has the master IP address configured. Alternatively, you can use the MAC address of the management port if the device has only one Routing Engine.

- Related Documentation**
- [Complete SNMPv3 Configuration Statements on page 1500](#)
 - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
 - [Example: SNMPv3 Configuration on page 1503](#)

Creating SNMPv3 Users

For each SNMPv3 user, you can specify the username, authentication type, authentication password, privacy type, and privacy password. After a user enters a password, a key based on the engine ID and password is generated and is written to the configuration file. After the generation of the key, the password is deleted from this configuration file.



NOTE: You can configure only one encryption type for each SNMPv3 user.

To create users, include the **user** statement at the **[edit snmp v3 usm local-engine]** hierarchy level:

```
[edit snmp v3 usm local-engine]
user username;
```

username is the name that identifies the SNMPv3 user.

To configure user authentication and encryption, include the following statements at the **[edit snmp v3 usm local-engine user username]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-md5 {
    authentication-password authentication-password;
}
authentication-sha {
    authentication-password authentication-password;
}
authentication-none;
privacy-aes128 {
    privacy-password privacy-password;
}
privacy-des {
    privacy-password privacy-password;
}
privacy-3des {
    privacy-password privacy-password;
}
privacy-none;
```

- Related Documentation**
- [Complete SNMPv3 Configuration Statements on page 1500](#)
 - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
 - [Example: Creating SNMPv3 Users on page 1508](#)
 - [Example: SNMPv3 Configuration on page 1503](#)

Example: Creating SNMPv3 Users

Define SNMPv3 users:

```
[edit]
snmp {
  v3 {
    usm {
      local-engine {
        user user1 {
          authentication-md5 {
            authentication-password authentication-password;
          }
          privacy-des {
            privacy-password password;
          }
        }
        user user2 {
          authentication-sha {
            authentication-password authentication-password;
          }
          privacy-none;
        }
        user user3 {
          authentication-none;
          privacy-none;
        }
        user user4 {
          authentication-md5 {
            authentication-password authentication-password;
          }
          privacy-des {
            privacy-password authentication-password;
          }
        }
        user user5 {
          authentication-sha {
            authentication-password authentication-password;
          }
          privacy-aes128 {
            privacy-password authentication-password;
          }
        }
      }
    }
  }
}
```

Related Documentation

- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the SNMPv3 Authentication Type

By default, in a Junos OS configuration the SNMPv3 authentication type is set to none.

This topic includes the following sections:

- [Configuring MD5 Authentication on page 1509](#)
- [Configuring SHA Authentication on page 1509](#)
- [Configuring No Authentication on page 1510](#)

Configuring MD5 Authentication

To configure the message digest algorithm (MD5) as the authentication type for an SNMPv3 user, include the **authentication-md5** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]  
authentication-md5 {  
    authentication-password authentication-password;  
}
```

authentication-password is the password used to generate the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring SHA Authentication

To configure the secure hash algorithm (SHA) as the authentication type for an SNMPv3 user, include the **authentication-sha** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]  
authentication-sha {  
    authentication-password authentication-password;  
}
```

authentication-password is the password used to generate the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring No Authentication

To configure no authentication for an SNMPv3 user, include the **authentication-none** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]  
authentication-none;
```

Related Documentation

- [Configuring the SNMPv3 Encryption Type on page 1510](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring the Access Privileges Granted to a Group on page 1513](#)
- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the SNMPv3 Encryption Type

By default, encryption is set to none.



NOTE: Before you configure encryption, you must configure MD5 or SHA authentication.

Before you configure the **privacy-des**, **privacy-3des** and **privacy-aes128** statements, you must install the **jcrypto** package, and either restart the SNMP process or reboot the router.

This topic includes the following sections:

- [Configuring the Advanced Encryption Standard Algorithm on page 1510](#)
- [Configuring the Data Encryption Algorithm on page 1511](#)
- [Configuring Triple DES on page 1511](#)
- [Configuring No Encryption on page 1511](#)

Configuring the Advanced Encryption Standard Algorithm

To configure the Advanced Encryption Standard (AES) algorithm for an SNMPv3 user, include the **privacy-aes128** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]  
privacy-aes128 {  
  privacy-password privacy-password;  
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring the Data Encryption Algorithm

To configure the data encryption algorithm (DES) for an SNMPv3 user, include the **privacy-des** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-des {
  privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring Triple DES

To configure triple DES for an SNMPv3 user, include the **privacy-3des** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-3des {
  privacy-password privacy-password;
}
```

privacy-password is the password used to generate the key used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Configuring No Encryption

To configure no encryption for an SNMPv3 user, include the **privacy-none** statement at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
privacy-none;
```

Related Documentation

- [Configuring the SNMPv3 Authentication Type on page 1509](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Configuring the Access Privileges Granted to a Group on page 1513](#)
- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Defining Access Privileges for an SNMP Group

The SNMP version 3 (SNMPv3) uses the view-based access control model (VACM), which allows you to configure the access privileges granted to a group. Access is controlled by filtering the MIB objects available for a specific operation through a predefined view. You assign views to determine the objects that are visible for read, write, and notify operations for a particular group, using a particular context, a particular security model (v1, v2c, or usm), and particular security level (authenticated, privacy, or none). For information about how to configure views, see [“Configuring MIB Views” on page 1496](#).

You define user access to management information at the **[edit snmp v3 vacm]** hierarchy level. All access control within VACM operates on groups, which are collections of users as defined by USM, or community strings as defined in the SNMPv1 and SNMPv2c security models. The term **security-name** refers to these generic end users. The group to which a specific security name belongs is configured at the **[edit snmp v3 vacm security-to-group]** hierarchy level. That security name can be associated with a group defined at the **[edit snmp v3 vacm security-to-group]** hierarchy level. A group identifies a collection of SNMP users that share the same access policy. You then define the access privileges associated with a group at the **[edit snmp v3 vacm access]** hierarchy level. Access privileges are defined using views. For each group, you can apply different views depending on the SNMP operation; for example, read (**get**, **getNext**, or **getBulk**) write (**set**), notifications, the security level used (authentication, privacy, or none), and the security model (v1, v2c, or usm) used within an SNMP request.

You configure members of a group with the **security-name** statement. For v3 packets using USM, the security name is the same as the username. For SNMPv1 or SNMPv2c packets, the security name is determined based on the community string. Security names are specific to a security model. If you are also configuring VACM access policies for SNMPv1 or SNMPv2c packets, you must assign security names to groups for each security model (SNMPv1 or SNMPv2c) at the **[edit snmp v3 vacm security-to-group]** hierarchy level. You must also associate a security name with an SNMP community at the **[edit snmp v3 snmp-community community-index]** hierarchy level.

To configure the access privileges for an SNMP group, include statements at the **[edit snmp v3 vacm]** hierarchy level:

```
[edit snmp v3 vacm]
access {
  group group-name {
    (default-context-prefix | context-prefix context-prefix){
```



```

security-model (any | usm | v1 | v2c) {
  security-level (authentication | none | privacy) {
    notify-view view-name;
    read-view view-name;
    write-view view-name;
  }
}
}
}
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}

```

Related Documentation

- [Configuring the SNMPv3 Authentication Type on page 1509](#)
- [Configuring the Access Privileges Granted to a Group on page 1513](#)
- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the Access Privileges Granted to a Group

This topic includes the following sections:

- [Configuring the Group on page 1513](#)
- [Configuring the Security Model on page 1514](#)
- [Configuring the Security Level on page 1514](#)
- [Associating MIB Views with an SNMP User Group on page 1514](#)

Configuring the Group

To configure the access privileges granted to a group, include the **group** statement at the **[edit snmp v3 vacm access]** hierarchy level:

```

[edit snmp v3 vacm access]
group group-name;

```

group-name is a collection of SNMP users that belong to a common SNMP list that defines an access policy. Users belonging to a particular SNMP group inherit all access privileges granted to that group.

Configuring the Security Model

To configure the security model, include the **security-model** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix)]
security-model (any | usm | v1 | v2c);
```

- **any**—Any security model
- **usm**—SNMPv3 security model
- **v1**—SNMPv1 security model
- **v2c**—SNMPv2c security model

Configuring the Security Level

To configure the access privileges granted to packets with a particular security level, include the **security-level** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model (any
| usm | v1 | v2c)]
security-level (authentication | none | privacy);
```

- **none**—Provides no authentication and no encryption.
- **authentication**—Provides authentication but no encryption.
- **privacy**—Provides authentication and encryption.



NOTE: Access privileges are granted to all packets with a security level equal to or greater than that configured. If you are configuring the SNMPv1 or SNMPv2c security model, use **none** as your security level. If you are configuring the SNMPv3 security model (USM), use the **authentication**, **none**, or **privacy** security level.

Associating MIB Views with an SNMP User Group

MIB views define access privileges for members of a group. Separate views can be applied for each SNMP operation (read, write, and notify) within each security model (usm, v1, and v2c) and each security level (authentication, none, and privacy) supported by SNMP.

To associate MIB views with an SNMP user group, include the following statements at the `[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
  context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none
  | privacy)]
  notify-view view-name;
  read-view view-name;
  write-view view-name;
```



NOTE: You must associate at least one view (notify, read, or write) at the `[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` hierarchy level.

You must configure the MIB view at the `[edit snmp view view-name]` hierarchy level. For information about how to configure MIB views, see [“Configuring MIB Views” on page 1496](#).

This section describes the following topics related to this configuration:

- [Configuring the Notify View on page 1515](#)
- [Configuring the Read View on page 1515](#)
- [Configuring the Write View on page 1516](#)

Configuring the Notify View

To associate notify access with an SNMP user group, include the **notify-view** statement at the `[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
  context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none
  | privacy)]
  notify-view view-name;
```

view-name specifies the notify access, which is a list of notifications that can be sent to each user in an SNMP group. A view name cannot exceed 32 characters.

Configuring the Read View

To associate a read view with an SNMP group, include the **read-view** statement at the `[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
  context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none
  | privacy)]
  read-view view-name;
```

view-name specifies read access for an SNMP user group. A view name cannot exceed 32 characters.

Configuring the Write View

To associate a write view with an SNMP user group, include the **write-view** statement at the **[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]** hierarchy level:

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix
context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none
| privacy)]
write-view view-name;
```

view-name specifies write access for an SNMP user group. A view name cannot exceed 32 characters.

Related Documentation

- [Configuring the SNMPv3 Authentication Type on page 1509](#)
- [Defining Access Privileges for an SNMP Group on page 1512](#)
- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: Configuring the Access Privileges Granted to a Group on page 1516](#)

Example: Configuring the Access Privileges Granted to a Group

Define access privileges:

```
[edit snmp v3]
access {
  group group1 {
    default-context-prefix {
      security-model usm {          #Define an SNMPv3 security model
        security-level privacy {
          notify-view nv1;
          read-view rv1;
          write-view wv1;
        }
      }
    }
  }
  context-prefix lr1/ri1 { # routing instance ri1 in logical system lr1
    security-model usm {
      security-level privacy {
        notify-view nv1;
        read-view rv1;
        write-view wv1;
      }
    }
  }
}
```

```

group group2 {
  default-context-prefix {
    security-model usm {      #Define an SNMPv3 security model
      security-level authentication {
        read-view rv2;
        write-view wv2;
      }
    }
  }
}
group group3 {
  default-context-prefix {
    security-model v1 {      #Define an SNMPv3 security model
      security-level none {
        read-view rv3;
        write-view wv3;
      }
    }
  }
}

```

Related Documentation

- [Configuring the Access Privileges Granted to a Group on page 1513](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Assigning Security Model and Security Name to a Group

To assign security names to groups, include the following statements at the **[edit snmp v3 vacm security-to-group]** hierarchy level:

```

[edit snmp v3 vacm security-to-group]
security-model (usm | v1 | v2c) {
  security-name security-name {
    group group-name;
  }
}

```

This topic includes the following sections:

- [Configuring the Security Model on page 1517](#)
- [Assigning Security Names to Groups on page 1518](#)
- [Configuring the Group on page 1518](#)

Configuring the Security Model

To configure the security model, include the **security-model** statement at the **[edit snmp v3 vacm security-to-group]** hierarchy level:

```

[edit snmp v3 vacm security-to-group]
security-model (usm | v1 | v2c);

```

- **usm**—SNMPv3 security model

- **v1**—SNMPv1 security model
- **v2c**—SNMPv2 security model

Assigning Security Names to Groups

To associate a security name with an SNMPv3 user, or a v1 or v2 community string, include the **security-name** statement at the **[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]** hierarchy level:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
  security-name security-name;
```

For SNMPv3, the **security-name** is the username configured at the **[edit snmp v3 usm local-engine user username]** hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the **[edit snmp v3 snmp-community community-index]** hierarchy level. For information about configuring usernames, see [“Creating SNMPv3 Users” on page 1507](#). For information about configuring a community string, see [“Configuring the SNMPv3 Community” on page 1536](#).



NOTE: The USM security name is separate from the SNMPv1 and SNMPv2c security name. If you support SNMPv1 and SNMPv2c in addition to SNMPv3, you must configure separate security names within the security-to-group configuration at the **[edit snmp v3 vacm access]** hierarchy level.

Configuring the Group

After you have created SNMPv3 users, or v1 or v2 security names, you associate them with a group. A group is a set of security names belonging to a particular security model. A group defines the access rights for all users belonging to it. Access rights define what SNMP objects can be read, written to, or created. A group also defines what notifications a user is allowed to receive.

If you already have a group that is configured with all of the view and access permissions that you want to give a user, you can add the user to that group. If you want to give a user view and access permissions that no other groups have, or if you do not have any groups configured, create a group and add the user to it.

To configure the access privileges granted to a group, include the **group** statement at the **[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name security-name]** hierarchy level:

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name
  security-name]
  group group-name;
```

group-name identifies a collection of SNMP security names that share the same access policy. For more information about groups, see [“Defining Access Privileges for an SNMP Group” on page 1512](#).

Example: Security Group Configuration

Assign security names to groups:

```
vacm {
  security-to-group {
    security-model usm {
      security-name user1 {
        group group1;
      }
      security-name user2 {
        group group2;
      }
      security-name user3 {
        group group3;
      }
    }
  }
}
```

Related Documentation

- [Assigning Security Model and Security Name to a Group on page 1517](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring SNMPv3 Traps on a Device Running Junos OS

In SNMPv3, you create traps and informs by configuring the **notify**, **target-address**, and **target-parameters** parameters. Traps are unconfirmed notifications, whereas informs are confirmed notifications. This section describes how to configure SNMP traps. For information about configuring SNMP informs, see [“Configuring SNMP Informs” on page 1529](#).

The target address defines a management application’s address and parameters to be used in sending notifications. Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target. SNMPv3 also lets you define SNMPv1 and SNMPv2c traps.



NOTE: When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Access privileges are configured at the `[edit snmp v3 vacm access]` and `[edit snmp v3 vacm security-to-group]` hierarchy levels.

To configure SNMP traps, include the following statements at the `[edit snmp v3]` hierarchy level:

```
[edit snmp v3]
  notify name {
    tag tag-name;
    type trap;
  }
```

```
notify-filter name {  
    oid object-identifier (include | exclude);  
}  
target-address target-address-name {  
    address address;  
    address-mask address-mask;  
    logical-system logical-system;  
    port port-number;  
    routing-instance instance;  
    tag-list tag-list;  
    target-parameters target-parameters-name;  
}  
target-parameters target-parameters-name {  
    notify-filter profile-name;  
    parameters {  
        message-processing-model (v1 | v2c | v3);  
        security-level (authentication | none | privacy);  
        security-model (usm | v1 | v2c);  
        security-name security-name;  
    }  
}
```

**Related
Documentation**

- [Configuring the SNMPv3 Trap Notification on page 1520](#)
- [Configuring the Trap Notification Filter on page 1522](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Configuring SNMP Informs on page 1529](#)
- [Configuring the Remote Engine and Remote User on page 1530](#)
- [Configuring the Inform Notification Type and Target Address on page 1534](#)

Configuring the SNMPv3 Trap Notification

The **notify** statement specifies the type of notification (trap) and contains a single tag. The tag defines a set of target addresses to receive a trap. The tag list contains one or more tags and is configured at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level. If the tag list contains this tag, Junos OS sends a notification to all the target addresses associated with this tag.

To configure the trap notifications, include the **notify** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]  
notify name {  
    tag tag-name;  
    type trap;  
}
```

name is the name assigned to the notification.

tag-name defines the target addresses to which this notification is sent. This notification is sent to all the target-addresses that have this tag in their tag list. The **tag-name** is not included in the notification.

trap is the type of notification.



NOTE: Each notify entry name must be unique.

Junos OS supports two types of notification: **trap** and **inform**.

For information about how to configure the tag list, see “Configuring the Trap Target Address” on page 1524.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the Trap Notification Filter on page 1522](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Configuring SNMP Informs on page 1529](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Example: Configuring SNMPv3 Trap Notification

Specify three sets of destinations to send traps:

```
[edit snmp v3]
notify n1 {
  tag router1;
  type trap;
}
notify n2 {
  tag router2;
  type trap;
}
notify n3 {
  tag router3;
  type trap;
}
```

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the Trap Notification Filter

SNMPv3 uses the notify filter to define which traps (or which objects from which traps) are sent to the network management system (NMS). The trap notification filter limits the type of traps that are sent to the NMS.

Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). You can also use the wildcard character asterisk (*) in the object identifier (OID) to specify object identifiers that match a particular pattern.

To configure the trap notifications filter, include the **notify-filter** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
  notify-filter profile-name;
```

profile-name is the name assigned to the notify filter.

By default, the OID is set to **include**. To define access to traps (or objects from traps), include the **oid** statement at the **[edit snmp v3 notify-filter *profile-name*]** hierarchy level:

```
[edit snmp v3 notify-filter profile-name]
  oid oid (include | exclude);
```

oid is the object identifier. All MIB objects represented by this statement have the specified OID as a prefix. It can be specified either by a sequence of dotted integers or by a subtree name.

- **include**—Include the subtree of MIB objects represented by the specified OID.
- **exclude**—Exclude the subtree of MIB objects represented by the specified OID.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the SNMPv3 Trap Notification on page 1520](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Configuring SNMP Informs on page 1529](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the Trap Target Address

The target address defines a management application's address and parameters that are used in sending notifications. It can also identify management stations that are allowed to use specific community strings. When you receive a packet with a recognized community string and a tag is associated with it, Junos OS looks up all the target addresses

with this tag and verifies that the source address of this packet matches one of the configured target addresses.



NOTE: You must configure the address mask when you configure the SNMP community.

To specify where you want the traps to be sent and define what SNMPv1 and SNMPv2cc packets are allowed, include the **target-address** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
  target-address target-address-name;
```

target-address-name is the string that identifies the target address.

To configure the target address properties, include the following statements at the **[edit snmp v3 target-address target-address-name]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
  address address;
  address-mask address-mask;
  logical-system logical-system;
  port port-number;
  routing-instance instance;
  tag-list tag-list;
  target-parameters target-parameters-name;
```

This section includes the following topics:

- [Configuring the Address on page 1523](#)
- [Configuring the Address Mask on page 1523](#)
- [Configuring the Port on page 1524](#)
- [Configuring the Routing Instance on page 1524](#)
- [Configuring the Trap Target Address on page 1524](#)
- [Applying Target Parameters on page 1525](#)

Configuring the Address

To configure the address, include the **address** statement at the **[edit snmp v3 target-address target-address-name]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]
  address address;
```

address is the SNMP target address.

Configuring the Address Mask

The address mask specifies a set of addresses that are allowed to use a community string and verifies the source addresses for a group of target addresses.

To configure the address mask, include the **address-mask** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]  
  address-mask address-mask;
```

address-mask combined with the address defines a range of addresses. For information about how to configure the community string, see [“Configuring the SNMPv3 Community” on page 1536](#).

Configuring the Port

By default, the UDP port is set to 162. To configure a different port number, include the **port** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]  
  port port-number;
```

port-number is the SNMP target port number.

Configuring the Routing Instance

Traps are sent over the default routing instance. To configure the routing instance for sending traps, include the **routing-instance** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]  
  routing-instance instance;
```

instance is the name of the routing instance. To configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (/) to separate the two names (for example, **test-lr/test-ri**). To configure the default routing instance on a logical system, specify the logical system name followed by **default** (for example, **test-lr/default**).

Configuring the Trap Target Address

Each **target-address** statement can have one or more tags configured in its tag list. Each tag can appear in more than one tag list. When a significant event occurs on the network device, the tag list identifies the targets to which a notification is sent.

To configure the tag list, include the **tag-list** statement at the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
[edit snmp v3 target-address target-address-name]  
  tag-list "tag-list";
```

tag-list specifies one or more tags as a space-separated list enclosed within double quotes.

For an example of tag list configuration, see [“Example: Configuring the Tag List” on page 1525](#).

For information about how to specify a tag at the **[edit snmp v3 notify *notify-name*]** hierarchy level, see [“Configuring the SNMPv3 Trap Notification” on page 1520](#).



NOTE: When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Configure access privileges at the `[edit snmp v3 vacm access]` hierarchy level.

Applying Target Parameters

The `target-parameters` statement at the `[edit snmp v3]` hierarchy level applies the target parameters configured at the `[edit snmp v3 target-parameters target-parameters-name]` hierarchy level.

To reference configured target parameters, include the `target-parameters` statement at the `[edit snmp v3 target-address target-address-name]` hierarchy level:

```
[edit snmp v3 target-address target-address-name]
  target-parameters target-parameters-name;
```

target-parameters-name is the name associated with the message processing and security parameters that are used in sending notifications to a particular management target.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the SNMPv3 Trap Notification on page 1520](#)
- [Configuring the Trap Notification Filter on page 1522](#)
- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Configuring SNMP Informs on page 1529](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: Configuring the Tag List on page 1525](#)

Example: Configuring the Tag List

In the following example, two tag entries (**router1** and **router2**) are defined at the `[edit snmp v3 notify notify-name]` hierarchy level. When an event triggers a notification, Junos OS sends a trap to all target addresses that have **router1** or **router2** configured in their target-address tag list. This results in the first two targets getting one trap each, and the third target getting two traps.

```
[edit snmp v3]
  notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap; # Defines the type of notification
  }
  notify n2 {
    tag router2;
    type trap;
  }
  target-address ta1 {
    address 10.1.1.1;
```

```

    address-mask 255.255.255.0;
    port 162;
    tag-list router1;
    target-parameters tp1;
  }
  target-address ta2 {
    address 10.1.1.2;
    address-mask 255.255.255.0;
    port 162;
    tag-list router2;
    target-parameters tp2;
  }
  target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list "router1 router2"; #Define multiple tags in the target address tag list
    target-parameters tp3;
  }

```

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Defining and Configuring the Trap Target Parameters

Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target.

To define a set of target parameters, include the **target-parameters** statement at the **[edit snmp v3]** hierarchy level:

```

[edit snmp v3]
  target-parameters target-parameters-name;

```

target-parameters-name is the name assigned to the target parameters.

To configure target parameter properties, include the following statements at the **[edit snmp v3 target-parameters target-parameter-name]** hierarchy level:

```

[edit snmp v3 target-parameters target-parameter-name]
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | V3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }

```

This topic includes the following sections:

- [Applying the Trap Notification Filter on page 1527](#)
- [Configuring the Target Parameters on page 1527](#)

Applying the Trap Notification Filter

To apply the trap notification filter, include the **notify-filter** statement at the **[edit snmp v3 target-parameters *target-parameter-name*]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name]  
  notify-filter profile-name;
```

profile-name is the name of a configured notify filter. For information about configuring notify filters, see “[Configuring the Trap Notification Filter](#)” on page 1522.

Configuring the Target Parameters

To configure target parameter properties, include the following statements at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]  
  message-processing-model (v1 | v2c | v3);  
  security-level (authentication | none | privacy);  
  security-model (usm | v1 | v2c);  
  security-name security-name;
```

This section includes the following topics:

- [Configuring the Message Processing Model on page 1527](#)
- [Configuring the Security Model on page 1528](#)
- [Configuring the Security Level on page 1528](#)
- [Configuring the Security Name on page 1528](#)

Configuring the Message Processing Model

The message processing model defines which version of SNMP to use when generating SNMP notifications. To configure the message processing model, include the **message-processing-model** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]  
  message-processing-model (v1 | v2c | v3);
```

- **v1**—SNMPv1 message processing model
- **v2c**—SNMPv2c message processing model
- **v3**—SNMPv3 message processing model

Configuring the Security Model

To define the security model to use when generating SNMP notifications, include the **security-model** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
  security-model (usm | v1 | v2c);
```

- **usm**—SNMPv3 security model
- **v1**—SNMPv1 security model
- **v2c**—SNMPv2c security model

Configuring the Security Level

The **security-level** statement specifies whether the trap is authenticated and encrypted before it is sent.

To configure the security level to use when generating SNMP notifications, include the **security-level** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
  security-level (authentication | none | privacy);
```

- **authentication**—Provides authentication but no encryption.
- **none**—No security. Provides no authentication and no encryption.
- **privacy**—Provides authentication and encryption.



NOTE: If you are configuring the SNMPv1 or SNMPv2c security model, use **none** as your security level. If you are configuring the SNMPv3 (USM) security model, use the **authentication** or **privacy** security level.

Configuring the Security Name

To configure the security name to use when generating SNMP notifications, include the **security-name** statement at the **[edit snmp v3 target-parameters *target-parameter-name* parameters]** hierarchy level:

```
[edit snmp v3 target-parameters target-parameter-name parameters]
  security-name security-name;
```

If the USM security model is used, the **security-name** identifies the user that is used when the notification is generated. If the v1 or v2c security models are used, **security-name** identifies the SNMP community used when the notification is generated.



NOTE: The access privileges for the group associated with a security name must allow this notification to be sent.

If you are using the v1 or v2 security models, the security name at the [edit snmp v3 vacm security-to-group] hierarchy level must match the security name at the [edit snmp v3 snmp-community *community-index*] hierarchy level.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring the SNMPv3 Trap Notification on page 1520](#)
- [Configuring the Trap Notification Filter on page 1522](#)
- [Configuring the Trap Target Address on page 1522](#)
- [Configuring SNMP Informs on page 1529](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring SNMP Informs

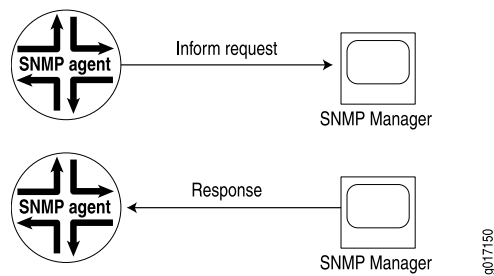
Junos OS supports two types of notifications: traps and informs. With traps, the receiver does not send any acknowledgment when it receives a trap. Therefore, the sender cannot determine if the trap was received. A trap may be lost because a problem occurred during transmission. To increase reliability, an inform is similar to a trap except that the inform is stored and retransmitted at regular intervals until one of these conditions occurs:

- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted and the agent discards the inform message.

If the sender never receives a response, the inform can be sent again. Thus, informs are more likely to reach their intended destination than traps are. Informs use the same communications channel as traps (same socket and port) but have different protocol data unit (PDU) types.

Informs are more reliable than traps, but they consume more network, router, and switch resources (see [Figure 33](#)). Unlike a trap, an inform is held in memory until a response is received or the timeout is reached. Also, traps are sent only once, whereas an inform may be retried several times. Use informs when it is important that the SNMP manager receive all notifications. However, if you are more concerned about network traffic, or router and switch memory, use traps.

Figure 33: Inform Request and Response



For information about configuring SNMP traps, see [“Configuring SNMPv3 Traps on a Device Running Junos OS”](#) on page 1519.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS](#) on page 1519
- [Configuring the Remote Engine and Remote User](#) on page 1530
- [Configuring the Inform Notification Type and Target Address](#) on page 1534
- [Complete SNMPv3 Configuration Statements](#) on page 1500
- [Minimum SNMPv3 Configuration on a Device Running Junos OS](#) on page 1502

Configuring the Remote Engine and Remote User

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. When sending an inform message, the agent uses the credentials of the user configured on the remote engine (inform target).

To configure a remote engine and remote user to receive and respond to SNMP informs, include the following statements at the `[edit snmp v3]` hierarchy level:

```

[edit snmp v3]
usm {
  remote-engine engine-id {
    user username {
      authentication-md5 {
        authentication-key key;
      }
      authentication-none;
      authentication-sha {
        authentication-key key;
      }
      privacy-3des {
        privacy-key key;
      }
      privacy-aes128 {
        privacy-key key;
      }
      privacy-des {
        privacy-key key;
      }
    }
  }
}
  
```

```

        privacy-none;
    }
}

```

For informs, **remote-engine *engine-id*** is the identifier for the SNMP agent on the remote device where the user resides.

For informs, **user *username*** is the user on a remote SNMP engine who receives the informs.

Informs generated can be **unauthenticated**, **authenticated**, or **authenticated_and_encrypted**, depending on the security level of the SNMPv3 user configured on the remote engine (the inform receiver). The authentication key is used for generating message authentication code (MAC). The privacy key is used to encrypt the inform PDU part of the message.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring SNMP Informs on page 1529](#)
- [Configuring the Inform Notification Type and Target Address on page 1534](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: Configuring the Remote Engine ID and Remote User on page 1531](#)

Example: Configuring the Remote Engine ID and Remote User

This example shows how to configure a remote engine and remote user so you can receive and respond to SNMP inform notifications. Inform notifications can be authenticated and encrypted. They are also more reliable than traps, another type of notification that Junos OS supports. Unlike traps, inform notifications are stored and retransmitted at regular intervals until one of these conditions occurs:

- The target of the inform notification returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted.
- [Requirements on page 1531](#)
- [Overview on page 1532](#)
- [Configuration on page 1532](#)
- [Verification on page 1533](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

This feature requires the use of plain-text passwords valid for SNMPv3. SNMPv3 has the following special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Although quotation marks are not always required to enclose passwords, it is best to use them. You need quotation marks if the password contains any spaces or possibly in the case of certain special characters or punctuation.

Overview

Inform notifications are supported in SNMPv3 to increase reliability. For example, an SNMP agent receiving an inform notification acknowledges the receipt.

For inform notifications, the remote engine ID identifies the SNMP agent on the remote device where the user resides, and the username identifies the user on a remote SNMP engine who receives the inform notifications.

Consider a scenario in which you have the values in [Table 113](#) to use in configuring the remote engine ID and remote user in this example.

Table 113: Values to Use in Example

Name of Variable	Value
username	u10
remote engine ID	800007E5804089071BC6D10A41
authentication type	authentication-md5
authentication password	qol67R%?
encryption type	privacy-des
privacy password	m*72Jl9v

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into a text file, remove any line breaks and change any details necessary to match your network configuration, copy and paste these commands into the CLI at the **[edit snmp v3]** hierarchy level, and then enter **commit** from configuration mode.

```
set usm remote-engine 800007E5804089071BC6D10A41 user u10 authentication-md5
authentication-key "qol67R%?"
set usm remote-engine 800007E5804089071BC6D10A41 user u10 privacy-des privacy-key
"m*72Jl9v"
```

Configuring the Remote Engine and Remote User

Step-by-Step Procedure The following example requires that you navigate to various levels in the configuration hierarchy. For information about navigating the CLI, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *Junos OS CLI User Guide*.

To configure the remote engine ID and remote user:

1. Configure the remote engine ID, username, and authentication type and password.

```
[edit snmp v3]
user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10
authentication-md5 authentication-key "qol67R%?"
```

2. Configure the encryption type and privacy password.

You can configure only one encryption type per SNMPv3 user.

```
[edit snmp v3]
user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10
privacy-des privacy-key "m*72Jl9v"
```

Results

In configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit snmp v3]
user@ host# show
usm {
  remote-engine 800007E5804089071BC6D10A41 {
    user u10 {
      authentication-md5 {
        authentication-key "$9$Tz/teK8NdsLXk.f5n6p0ORev"; ## SECRET-DATA
      }
      privacy-des {
        privacy-key "$9$/gyNCu1KvWdwYMWw2gJHkRhcrWx"; ## SECRET-DATA
      }
    }
  }
}
```

After you have confirmed that the configuration is correct, enter **commit** from configuration mode.

Verification

Verifying the Configuration of the Remote Engine ID and Username

Purpose Verify the status of the engine ID and user information.

Action Display information about the SNMPv3 engine ID and user.

```
user@host> show snmp v3
Local engine ID: 80 00 0a 4c 01 0a ff 03 e3
Engine boots:      3
Engine time:       769187 seconds
Max msg size:      65507 bytes

Engine ID: 80 00 07 e5 80 40 89 07 1b c6 d1 0a 41
  User                               Auth/Priv  Storage  Status
  u10                               md5/des   nonvolatile active
```

Meaning The output displays the following information:

- Local engine ID and detail about the engine
- Remote engine ID (labeled **Engine ID**)
- Username
- Authentication type and encryption (privacy) type that is configured for the user
- Type of storage for the username, either nonvolatile (configuration saved) or volatile (not saved)
- Status of the new user; only users with an active status can use SNMPv3

- Related Documentation**
- [show snmp v3 on page 2217](#)
 - [Configuring the SNMPv3 Encryption Type on page 1510](#)
 - [Configuring the SNMPv3 Authentication Type on page 1509](#)
 - [Configuring SNMP Informs on page 1529](#)
 - [Configuring the Remote Engine and Remote User on page 1530](#)

Configuring the Inform Notification Type and Target Address

To configure the inform notification type and target information, include the following statements at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify name {
  tag tag-name;
  type (trap | inform);
}
target-address target-address-name {
  address address;
  address-mask address-mask;
  logical-system logical-system;
  port port-number;
  retry-count number;
  routing-instance instance;
  tag-list tag-list;
  target-parameters target-parameters-name;
```

```

    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | v3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
}

```

notify *name* is the name assigned to the notification. Each notify entry name must be unique.

tag *tag-name* defines the target addresses that are sent this notification. The notification is sent to all target addresses that have this tag in their tag list. The **tag-name** is not included in the notification. For information about how to configure the tag list, see [“Configuring the Trap Target Address” on page 1524](#).

type *inform* is the type of notification.

target-address *target-address-name* identifies the target address. The target address defines a management application's address and parameters that are used to respond to informs.

timeout *seconds* is the number of seconds to wait for an acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted. The default timeout is **15** seconds.

retry-count *number* is the maximum number of times an inform is transmitted if no acknowledgment is received. The default is **3**. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.

message-processing-model defines which version of SNMP to use when SNMP notifications are generated. Informs require a **v3** message processing model.

security-model defines the security model to use when SNMP notifications are generated. Informs require a **usm** security model.

security-model defines the security model to use when SNMP notifications are generated. Informs require a **usm** security model.

security-level specifies whether the inform is authenticated and encrypted before it is sent. For the **usm** security model, the security level must be one of the following:

- **authentication**—Provides authentication but no encryption.
- **privacy**—Provides authentication and encryption.

security-name identifies the username that is used when generating the inform.

Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1519](#)
- [Configuring SNMP Informs on page 1529](#)

- [Configuring the Remote Engine and Remote User on page 1530](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1536](#)

Example: Configuring the Inform Notification Type and Target Address

In the following example, target **172.17.20.184** is configured to respond to informs. The inform timeout is **30** seconds and the maximum retransmit count is **3**. The inform is sent to all targets in the **tl1** list. The security model for the remote user is **usm** and the remote engine username is **u10**.

```
[edit snmp v3]
  notify n1 {
    type inform;
    tag tl1;
  }
  notify-filter nf1 {
    oid .1.3 include;
  }
  target-address ta1 {
    address 172.17.20.184;
    retry-count 3;
    tag-list tl1;
    address-mask 255.255.255.0;
    target-parameters tp1;
    timeout 30;
  }
  target-parameters tp1 {
    parameters {
      message-processing-model v3;
      security-model usm;
      security-level privacy;
      security-name u10;
    }
    notify-filter nf1;
  }
```

Related Documentation

- [Configuring the Inform Notification Type and Target Address on page 1534](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring the SNMPv3 Community

The SNMP community defines the relationship between an SNMP server system and the client systems. This statement is optional.

To configure the SNMP community, include the **snmp-community** statement at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
snmp-community community-index;
```

community-index is the index for the SNMP community.

To configure the SNMP community properties, include the following statements at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
community-name community-name;
context context-name;
security-name security-name;
tag tag-name;
```

This section includes the following topics:

- [Configuring the Community Name on page 1537](#)
- [Configuring the Context on page 1538](#)
- [Configuring the Security Names on page 1538](#)
- [Configuring the Tag on page 1538](#)

Configuring the Community Name

The community name defines the SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2c clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (read, write, or notify) allowed on those objects.

To configure the SNMP community name, include the **community-name** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
community-name community-name;
```

community-name is the community string for an SNMPv1 or SNMPv2c community.

If unconfigured, it is the same as the community index.

If the community name contains spaces, enclose it in quotation marks (" ").



NOTE: Community names must be unique. You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community community-index]** hierarchy levels. The configured community name at the **[edit snmp v3 snmp-community community-index]** hierarchy level is encrypted. You cannot view the community name after you have configured it and committed your changes. In the command-line interface (CLI), the community name is concealed.

Configuring the Context

An SNMP context defines a collection of management information that is accessible to an SNMP entity. Typically, an SNMP entity has access to multiple contexts. A context can be a physical or logical system, a collection of multiple systems, or even a subset of a system. Each context in a management domain has a unique identifier.

To configure an SNMP context, include the **context context-name** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
context context-name;
```



NOTE: To query a routing instance or a logical system,

Configuring the Security Names

To assign a community string to a security name, include the **security-name** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
security-name security-name;
```

security-name is used when access control is set up. The **security-to-group** configuration at the **[edit snmp v3 vacm]** hierarchy level identifies the group.



NOTE: This security name must match the security name configured at the **[edit snmp v3 target-parameters target-parameters-name parameters]** hierarchy level when you configure traps.

Configuring the Tag

To configure the tag, include the **tag** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
tag tag-name;
```

tag-name identifies the address of managers that are allowed to use a community string.

Related Documentation

- [Creating SNMPv3 Users on page 1507](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)
- [Example: Configuring an SNMPv3 Community on page 1539](#)

Example: Configuring an SNMPv3 Community

Define an SNMP community:

```
[edit snmp v3]
snmp-community index1 {
  community-name "$9$JOZl.QF/AtOz3"; # SECRET-DATA
  security-name john;
  tag router1; # Identifies managers that are allowed to use
  # a community string
  target-address ta1 {
    address 10.1.1.1;
    address-mask 255.255.255.0; # Defines the range of addresses
    port 162;
    tag-list router1;
    target-parameters tp1; # Applies configured target parameters
  }
}
```

**Related
Documentation**

- [Configuring the SNMPv3 Community on page 1536](#)
- [Complete SNMPv3 Configuration Statements on page 1500](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502](#)

Configuring SNMP for Routing Instances

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [SNMP MIBs Supported for Routing Instances on page 1542](#)
- [Support Classes for MIB Objects on page 1552](#)
- [SNMP Traps Supported for Routing Instances on page 1553](#)
- [Identifying a Routing Instance on page 1554](#)
- [Enabling SNMP Access over Routing Instances on page 1555](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1556](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1557](#)

Understanding SNMP Support for Routing Instances

Junos OS enables SNMP managers for all routing instances to request and manage SNMP data related to the corresponding routing instances and logical system networks.

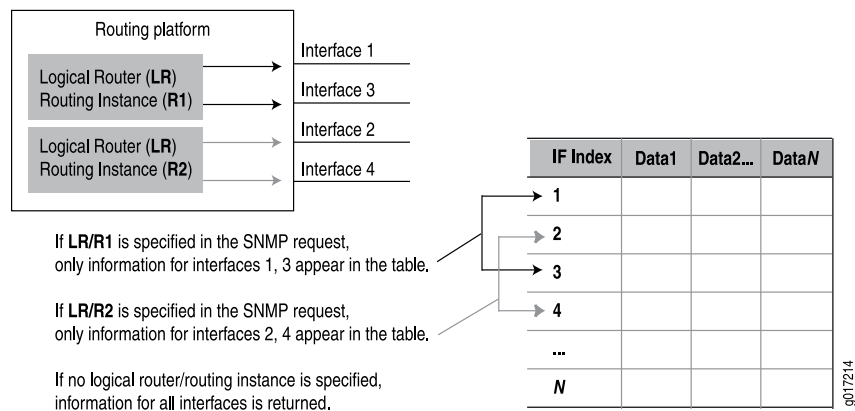
In Junos OS:

- Clients from routing instances other than the default can access MIB objects and perform SNMP operations only on the logical system networks to which they belong.
- Clients from the default routing instance can access information related to all routing instances and logical system networks.

Before Junos OS Release 8.4, only the SNMP manager in the default routing instance (**inet.0**) had access to the MIB objects

With the increase in virtual private network (VPN) service offerings, this feature is useful particularly for service providers who need to obtain SNMP data for specific routing instances (see [Figure 34](#)). Service providers can use this information for their own management needs or export the data for use by their customers.

Figure 34: SNMP Data for Routing Instances



If no routing instance is specified in the request, the SNMP agent operates as before:

- For nonrouting table objects, all instances are exposed.
- For routing table objects, only those associated with the default routing instance are exposed.



NOTE: The actual protocol data units (PDUs) are still exchanged over the default (inet.0) routing instance, but the data contents returned are dictated by the routing instance specified in the request PDUs.

Related Documentation

- [Support Classes for MIB Objects on page 1552](#)
- [SNMP Traps Supported for Routing Instances on page 1553](#)
- [Identifying a Routing Instance on page 1554](#)
- [Enabling SNMP Access over Routing Instances on page 1555](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1557](#)

SNMP MIBs Supported for Routing Instances

Table 114 shows enterprise-specific MIB objects supported by Junos OS and provides notes detailing how they are handled when a routing instance is specified in an SNMP request. An en dash (–) indicates that the item is not applicable.

Table 114: MIB Support for Routing Instances (Juniper Networks MIBs)

Object	Support Class	Description/Notes
jnxProducts(1)	–	Product Object IDs
jnxServices(2)	–	Services

Table 114: MIB Support for Routing Instances (Juniper Networks MIBs) (*continued*)

Object	Support Class	Description/Notes
jnxMibs(3) jnxBoxAnatomy(1)	Class 3	Objects are exposed only for the default logical system.
mpls(2)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
ifJnx(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAlarms(4)	Class 3	Objects are exposed only for the default logical system.
jnxFirewalls(5)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxDCUs(6)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxPingMIB(7)	Class 3	Objects are exposed only for the default logical system.
jnxTraceRouteMIB(8)	Class 3	Objects are exposed only for the default logical system.
jnxATM(10)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxIpv6(11)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxIpv4(12)	Class 1	jnxIpv4AddrTable(1) . Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxRmon(13)	Class 3	jnxRmonAlarmTable(1) . Objects are exposed only for the default logical system.
jnxLdp(14)	Class 2	jnxLdpTrapVars(1) . All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.

Table 114: MIB Support for Routing Instances (Juniper Networks MIBs) (continued)

Object	Support Class	Description/Notes
jnxCos(15) jnxCosIfqStatsTable(1) jnxCosFcTable(2) jnxCosFcIdTable(3) jnxCosQstatTable(4)	Class 3	Objects are exposed only for the default logical system.
jnxScu(16) jnxScuStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxRpf(17) jnxRpfStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxCfgMgmt(18)	Class 3	Objects are exposed only for the default logical system.
jnxPMon(19) jnxPMonFlowTable(1) jnxPMonErrorTable(2) jnxPMonMemoryTable(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxSonet(20) jnxSonetAlarmTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAtmCos(21) jnxCosAtmVcTable(1) jnxCosAtmScTable(2) jnxCosAtmVcQstatsTable(3) jnxCosAtmTrunkTable(4)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
ipSecFlowMonitorMIB(22)	–	–
jnxMac(23) jnxMacStats(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
apsMIB(24)	Class 3	Objects are exposed only for the default logical system.
jnxChassisDefines(25)	Class 3	Objects are exposed only for the default logical system.

Table 114: MIB Support for Routing Instances (Juniper Networks MIBs) (continued)

Object	Support Class	Description/Notes
jnxVpnMIB(26)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
jnxSericesInfoMib(27)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxCollectorMIB(28)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxHistory(29)	—	—
jnxSpMIB(32)	Class 3	Objects are exposed only for the default logical system.

[Table 115](#) shows Class 1 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 1 objects, only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.

Table 115: Class 1 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 1	802.3ad.mib	(dot3adAgg) MIB objects: dot3adAggTable dot3adAggPortListTable (dot3adAggPort) dot3adAggPortTable dot3adAggPortStatsTable dot3adAggPortDebugTable
	rfc2863a.mib	ifTable ifXTable ifStackTable
	rfc2011a.mib	ipAddrTable ipNetToMediaTable
	rtmib.mib	ipForward (ipCidrRouteTable)
	rfc2665a.mib	dot3StatsTable dot3ControlTable dot3PauseTable
	rfc2495a.mib	dsx1ConfigTable dsx1CurrentTable dsx1IntervalTable dsx1TotalTable dsx1FarEndCurrentTable dsx1FarEndIntervalTable dsx1FarEndTotalTable dsx1FracTable ...
	rfc2496a.mib	dsx3 (dsx3ConfigTable)
	rfc2115a.mib	frDlcmiTable (and related MIB objects)
	rfc3592.mib	sonetMediumTable (and related MIB objects)

Table 115: Class 1 MIB Objects (Standard and Juniper MIBs) (*continued*)

Class	MIB	Objects
	rfc3020.mib	mfrMIB mfrBundleTable mfrMibBundleLinkObjects mfrBundleIfIndexMappingTable (and related MIB objects)
	ospf2mib.mib	All objects
	ospf2trap.mib	All objects
	bgpmib.mib	All objects
	rfc2819a.mib	Example: etherStatsTable

Table 115: Class 1 MIB Objects (Standard and Juniper MIBs) (*continued*)

Class	MIB	Objects
Class 1	rfc2863a.mib	Examples: ifXtable ifStackTable
	rfc2665a.mib	etherMIB
	rfc2515a.mib	atmMIB objects Examples: atmInterfaceConfTable atmVplTable atmVclTable
	rfc2465.mib	ip-v6mib Examples: ipv6IfTable ipv6AddrPrefixTable ipv6NetToMediaTable ipv6RouteTable
	rfc2787a.mib	vrrp mib
	rfc2932.mib	ipMRouteMIB ipMRouteStdMIB
	mroutemib.mib	ipMRoute1MIBObjects
	isismib.mib	isisMIB
	pimmib.mib	pimMIB
	msdpmib.mib	msdpmib
	jnx-if-extensions.mib	Examples: ifJnxTable ifChassisTable
	jnx-dcu.mib	jnxDCUs
	jnx-atm.mib	

Table 115: Class 1 MIB Objects (Standard and Juniper MIBs) (*continued*)

Class	MIB	Objects
		Examples: <code>jnxAtmIfTable</code> <code>jnxAtmVcTable</code> <code>jnxAtmVpTable</code>
	<code>jnx-ipv4.mib</code>	<code>jnxipv4</code> Example: <code>jnxIpv4AddrTable</code>
	<code>jnx-cos.mib</code>	Examples: <code>jnxCosIfqStatsTable</code> <code>jnxCosQstatTable</code>
	<code>jnx-scu.mib</code>	Example: <code>jnxScuStatsTable</code>
	<code>jnx-rpf.mib</code>	Example: <code>jnxRpfStatsTable</code>
	<code>jnx-pmon.mib</code>	Example: <code>jnxPMonFlowTable</code>
	<code>jnx-sonet.mib</code>	Example: <code>jnxSonetAlarmTable</code>
	<code>jnx-atm-cos.mib</code>	Examples: <code>jnxCosAtmVcTable</code> <code>jnxCosAtmVcScTable</code> <code>jnxCosAtmVcQstatsTable</code> <code>jnxCosAtmTrunkTable</code>
	<code>jnx-mac.mib</code>	Example: <code>jnxMacStatsTable</code>
	<code>jnx-services.mib</code>	Example: <code>jnxSvcFlowTableAggStatsTable</code>
Class 1	<code>jnx-coll.mib</code>	<code>jnxCollectorMIB</code> Examples: <code>jnxCollPicIfTable</code> <code>jnxCollFileEntry</code>

Table 116 shows Class 2 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 2 objects, all instances within a logical system are exposed. Data will not be segregated down to the routing instance level.

Table 116: Class 2 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 2	rfc3813.mib	mplsLsrStdMIB Examples: mplsInterfaceTable mplsInSegmentTable mplsOutSegmentTable mplsLabelStackTable mplsXCTable (and related MIB objects)
	igmpmib.mib	igmpStdMIB NOTE: The igmpmib.mib is the draft version of the IGMP Standard MIB in the experimental tree. Junos OS does not support the original IGMP Standard MIB.
	l3vpn.mib	mplsVpnMIB
	jnx-mpls.mib	Example: mplsLspList
	jnx-ldp.mib	jnxLdp Example: jnxLdpStatsTable
	jnx-vpn.mib	jnxVpnMIB
	jnx-bgp.mib	jnxBgpM2Experiment
	jnx-bgp-mib2.mib	jnxBgpM2Experiment

Table 117 shows Class 3 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 3, objects are exposed only for the default logical system.

Table 117: Class 3 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 3	rfc2819a.mib	rmonEvents alarmTable logTable eventTable agentxMIB
	rfc2925a.mib	pingmib
	rfc2925b.mib	tracerouteMIB
	jnxchassis.mib	jnxBoxAnatomy
	jnx-chassis-alarm.mib	jnxAlarms
	jnx-ping.mib	jnxPingMIB
	jnx-traceroute.mib	jnxTraceRouteMIB
	jnx-rmon.mib	jnxRmonAlarmTable
	jnx-cos.mib	Example: jnxCosFcTable
	jnx-cfgmgmt.mib	Example: jnxCfgMgmt
	jnx-sonetaps.mib	apsMIBObjects
	jnx-sp.mib	jnxSpMIB
	ggsn.mib	ejnmobileipABmib
	rfc1907.mib	snmpModules
	snmpModules	Examples: snmpMIB snmpFrameworkMIB

Table 118 shows Class 4 MIB objects (standard and enterprise-specific MIBs) supported by Junos OS. With Class 4 objects, data is not segregated by routing instance. All instances are exposed.

Table 118: Class 4 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 4	system	Example: sysORTable
	rfc2011a.mib	ip (ipDefaultTTL , ipInReceives) icmp
	rfc2012a.mib	tcp tcpConnTable ipv6TcpConnTable
	rfc2013a.mib	udp udpTable ipv6UdpTable
	rfc2790a.mib	hrSystem
	rfc2287a.mib	sysApplOBJ
	jnx-firewall.mib	jnxFirewalls
	jnx-ipv6.mib	jnxIpv6

- Related Documentation**
- [Understanding SNMP Support for Routing Instances on page 1541](#)
 - [Support Classes for MIB Objects on page 1552](#)
 - [SNMP Traps Supported for Routing Instances on page 1553](#)

Support Classes for MIB Objects

When a routing instance is specified, all routing-related MIB objects return data maintained by the routing instance in the request. For all other MIB objects, the data returned is segregated according to that routing instance. For example, only those interfaces assigned to that routing instance (for example, the logical interfaces [ifls] as well as their corresponding physical interfaces [ifds]) are exposed by the SNMP agent. Similarly, objects with an unambiguous attachment to an interface (for example, **addresses**) are segregated as well.

For those objects where the attachment is ambiguous (for example, objects in **sysApplMIB**), no segregation is done and all instances are visible in all cases.

Another category of objects is visible only when no logical system is specified (only within the default logical system) regardless of the routing instance within the default logical system. Objects in this category are Chassis MIB objects, objects in the SNMP group,

RMON alarm, event and log groups, Ping MIB objects, configuration management objects, and V3 objects.

In summary, to support routing instances, MIB objects fall into one of the following categories:

- Class 1—Data is segregated according to the routing instance in the request. This is the most granular of the segregation classes.
- Class 2—Data is segregated according to the logical system specified in the request. The same data is returned for all routing instances that belong to a particular logical system. Typically, this applies to routing table objects where it is difficult to extract routing instance information or where routing instances do not apply.
- Class 3—Data is exposed only for the default logical system. The same set of data is returned for all routing instances that belong to the default logical system. If you specify another logical system (not the default), no data is returned. Typically this class applies to objects implemented in subagents that do not monitor logical system changes and register their objects using only the default context (for example, Chassis MIB objects).
- Class 4—Data is not segregated by routing instance. The same data is returned for all routing instances. Typically, this applies to objects implemented in subagents that monitor logical system changes and register or deregister all their objects for each logical system change. Objects whose values cannot be segregated by routing instance fall into this class.

See “[SNMP MIBs Supported for Routing Instances](#)” on page 1542 for a list of the objects associated with each class.

**Related
Documentation**

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [SNMP Traps Supported for Routing Instances on page 1553](#)

SNMP Traps Supported for Routing Instances

You can restrict the trap receivers from receiving traps that are not related to the logical system networks to which they belong. To do this, include the **logical-system-trap-filter** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]  
logical-system-trap-filter;
```

If the **logical-system-trap-filter** statement is not included in the SNMP configuration, all traps are forwarded to the configured routing instance destinations. However, even when this statement is configured, the trap receiver associated with the default routing instance will receive all SNMP traps.

When configured under the trap-group object, all v1 and v2c traps that apply to routing instances (or interfaces belonging to a routing instance) have the routing instance name encoded in the community string. The encoding is identical to that used in request PDUs.

For traps configured under the v3 framework, the routing instance name is carried in the context field when the v3 message processing model has been configured. For other

message processing models (v1 or v2c), the routing instance name is not carried in the trap message header (and not encoded in the community string).

Related Documentation

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [Support Classes for MIB Objects on page 1552](#)
- [SNMP MIBs Supported for Routing Instances on page 1542](#)

Identifying a Routing Instance

With this feature, routing instances are identified by either the context field in v3 requests or encoded in the community string in v1 or v2c requests.

When encoded in a community string, the routing instance name appears first and is separated from the actual community string by the @ character.

To avoid conflicts with valid community strings that contain the @ character, the community is parsed only if typical community string processing fails. For example, if a routing instance named **RI** is configured, an SNMP request with **RI@public** is processed within the context of the **RI** routing instance. Access control (views, source address restrictions, access privileges, and so on) is applied according to the actual community string (the set of data after the @ character—in this case **public**). However, if the community string **RI@public** is configured, the protocol data unit (PDU) is processed according to that community and the embedded routing instance name is ignored.

Logical systems perform a subset of the actions of a physical router and have their own unique routing tables, interfaces, policies, and routing instances. When a routing instance is defined within a logical system, the logical system name must be encoded along with the routing instance using a slash (/) to separate the two. For example, if the routing instance **RI** is configured within the logical system **LS**, that routing instance must be encoded within a community string as **LS/RI@public**. When a routing instance is configured outside a logical system (within the default logical system), no logical system name (or / character) is needed.

Also, when a logical system is created, a default routing instance (named **default**) is always created within the logical system. This name should be used when querying data for that routing instance (for example, **LS/default@public**). For v3 requests, the name **logical system/routing instance** should be identified directly in the context field.



NOTE: To identify a virtual LAN (VLAN) spanning-tree instance (VSTP on MX Series 3D Universal Edge Routers), specify the routing instance name followed by a double colon (::) and the VLAN ID. For example, to identify VSTP instance for VLAN 10 in the global default routing instance, include **default::10@public** in the context (SNMPv3) or community (SNMPv1 or v2) string.

Related Documentation

- [Understanding SNMP Support for Routing Instances](#)

- [Enabling SNMP Access over Routing Instances on page 1555](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)

Enabling SNMP Access over Routing Instances

To enable SNMP managers in routing instances other than the default routing instance to access SNMP information, include the **routing-instance-access** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
routing-instance-access;
```

If this statement is not included in the SNMP configuration, SNMP managers from routing instances other than the default routing instance cannot access SNMP information.

Related Documentation

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [Identifying a Routing Instance on page 1554](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1557](#)

Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community

You can specify the routing instance along with the client information when you add a client to an SNMP community. To specify the routing instance to which a client belongs, include the **routing-instance** statement followed by the routing instance name and client information in the SNMP configuration.

The following example shows the configuration statement to add routing instance **test-ri** to SNMP community **community1**.



NOTE: Routing instances specified at the **[edit snmp community community-name]** hierarchy level are added to the default logical system in the community.

```
[edit snmp]
community community1 {
  clients {
    10.209.152.33/32;
  }
  routing-instance test-ri {
    clients {
      10.19.19.1/32;
    }
  }
}
```

If the routing instance is defined within a logical system, include the **routing-instance** statement at the **[edit snmp community *community-name* logical-system *logical-system-name*]** hierarchy level, as in the following example:

```
[edit snmp]
community community1 {
  clients {
    10.209.152.33/32;
  }
  logical-system test-LS {
    routing-instance test-ri {
      clients {
        10.19.19.1/32;
      }
    }
  }
}
```

**Related
Documentation**

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [Identifying a Routing Instance on page 1554](#)
- [Enabling SNMP Access over Routing Instances on page 1555](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1557](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1556](#)

Example: Configuring Interface Settings for a Routing Instance

This example shows an **802.3ad ae0** interface configuration allocated to a routing instance named **INFrtid**:

```
[edit chassis]
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
[edit interfaces ae0]
vlan-tagging;
aggregated-ether-options {
  minimum-links 2;
  link-speed 100m;
}
unit 0 {
  vlan-id 100;
  family inet {
    address 10.1.0.1/24;
  }
}
[edit interfaces fe-1/1/0]
fastether-options {
  802.3ad ae0;
}
[edit interfaces fe-1/1/1]
```

```

fastether-options {
  802.3ad ae0;
}
[edit routing-instances]
INFrt {
  instance-type virtual-router;
  interface fe-1/1/0.0;
  interface fe-1/1/1.0;
  interface fe-1/1/5.0;
  interface ae0.0;
  protocols {
    ospf {
      area 0.0.0.0 {
        interface all;
      }
    }
  }
}

```

The following **snmpwalk** command shows how to retrieve SNMP-related information from **router1** and the 802.3ae bundle interface belonging to routing instance **INFrt** with the SNMP community **public**:

```

router# snmpwalk -Os router1 INFrt@public dot3adAggTable
dot3adAggMACAddress.59 = 0:90:69:92:93:f0
dot3adAggMACAddress.65 = 0:90:69:92:93:f0
dot3adAggActorSystemPriority.59 = 0
dot3adAggActorSystemPriority.65 = 0
dot3adAggActorSystemID.59 = 0:0:0:0:0:0
dot3adAggActorSystemID.65 = 0:0:0:0:0:0
dot3adAggAggregateOrIndividual.59 = true(1)
dot3adAggAggregateOrIndividual.65 = true(1)
dot3adAggActorAdminKey.59 = 0
dot3adAggActorAdminKey.65 = 0
dot3adAggActorOperKey.59 = 0
dot3adAggActorOperKey.65 = 0
dot3adAggPartnerSystemID.59 = 0:0:0:0:0:0
dot3adAggPartnerSystemID.65 = 0:0:0:0:0:0
dot3adAggPartnerSystemPriority.59 = 0
dot3adAggPartnerSystemPriority.65 = 0
dot3adAggPartnerOperKey.59 = 0
dot3adAggPartnerOperKey.65 = 0
dot3adAggCollectorMaxDelay.59 = 0
dot3adAggCollectorMaxDelay.65 = 0

```

- Related Documentation**
- [Understanding SNMP Support for Routing Instances on page 1541](#)
 - [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)

Configuring Access Lists for SNMP Access over Routing Instances

You can create and maintain access lists to manage access to SNMP information. Access list configuration enables you to allow or deny SNMP access to clients of a specific routing instance.

The following example shows how to create an access list:

```
[edit snmp]
routing-instance-access {
  access-list {
    ri1 restrict;
    ls1/default;
    ls1/ri2;
    ls1*;
  }
}
```

The configuration given in the example:

- Restricts clients in **ri1** from accessing SNMP information.
- Allows clients in **ls1/default**, **ls1/ri2**, and all other routing instances with names starting with **ls1** to access SNMP information.

You can use the wildcard character (*) to represent a string in the routing instance name.



NOTE: You cannot restrict the SNMP manager of the default routing instance from accessing SNMP information.

**Related
Documentation**

- [Understanding SNMP Support for Routing Instances on page 1541](#)
- [Enabling SNMP Access over Routing Instances on page 1555](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555](#)

Configuring SNMP Remote Operations

- [SNMP Remote Operations Overview on page 1559](#)
- [Using the Ping MIB for Remote Monitoring Devices Running Junos OS on page 1562](#)
- [Starting a Ping Test on page 1562](#)
- [Monitoring a Running Ping Test on page 1564](#)
- [Gathering Ping Test Results on page 1567](#)
- [Stopping a Ping Test on page 1568](#)
- [Interpreting Ping Variables on page 1568](#)
- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Starting a Traceroute Test on page 1570](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Stopping a Traceroute Test on page 1577](#)
- [Interpreting Traceroute Variables on page 1578](#)

SNMP Remote Operations Overview

A SNMP remote operation is any process on the router that can be controlled remotely using SNMP. Junos OS currently provides support for two SNMP remote operations: the Ping MIB and Traceroute MIB, defined in RFC 2925. Using these MIBs, an SNMP client in the network management system (NMS) can:

- Start a series of operations on a router
- Receive notification when the operations are complete
- Gather the results of each operation

Junos OS also provides extended functionality to these MIBs in the Juniper Networks enterprise-specific extensions **jnxPingMIB** and **jnxTraceRouteMIB**. For more information about **jnxPingMIB** and **jnxTraceRouteMIB**, see *PING MIB* and *Traceroute MIB*.

This topic covers the following sections:

- [SNMP Remote Operation Requirements on page 1560](#)
- [Setting SNMP Views on page 1560](#)
- [Setting Trap Notification for Remote Operations on page 1561](#)
- [Using Variable-Length String Indexes on page 1561](#)
- [Enabling Logging on page 1562](#)

SNMP Remote Operation Requirements

To use SNMP remote operations, you should be experienced with SNMP conventions. You must also configure Junos OS to allow the use of the remote operation MIBs.

Setting SNMP Views

All remote operation MIBs supported by Junos OS require that the SNMP clients have read-write privileges. The default SNMP configuration of Junos OS does not provide clients with a community string with such privileges.

To set read-write privileges for an SNMP community string, include the following statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
community community-name {
  authorization authorization;
  view view-name;
}
view view-name {
  oid object-identifier (include | exclude);
}
```

Example: Setting SNMP Views

To create a community named **remote-community** that grants SNMP clients read-write access to the Ping MIB, **jnxPing** MIB, Traceroute MIB, and **jnxTraceRoute** MIB, include the following statements at the **[edit snmp]** hierarchy level:

```
snmp {
  view remote-view {
    oid 1.3.6.1.2.1.80 include; # pingMIB
    oid 1.3.6.1.4.1.2636.3.7 include; # jnxPingMIB
    oid 1.3.6.1.2.1.81 include; # traceRouteMIB
    oid 1.3.6.1.4.1.2636.3.8 include; # jnxTraceRouteMIB
  }
  community remote-community {
    view remote-view;
    authorization read-write;
  }
}
```

For more information about the **community** statement, see [“Configuring SNMP Communities” on page 1479](#) and [community \(SNMP\)](#).

For more information about the **view** statement, see [“Configuring MIB Views” on page 1496](#), [view \(Associating a MIB View with a Community\)](#), and [view \(Configuring a MIB View\)](#).

Setting Trap Notification for Remote Operations

In addition to configuring the remote operations MIB for trap notification, you must also configure Junos OS. You must specify a target host for remote operations traps.

To configure trap notification for SNMP remote operations, include the **categories** and **targets** statements at the **[edit snmp trap-group group-name]** hierarchy level:

```
[edit snmp trap-group group-name]
  categories {
    category;
  }
  targets {
    address;
  }
}
```

Example: Setting Trap Notification for Remote Operations

Specify 172.17.12.213 as a target host for all remote operation traps:

```
snmp {
  trap-group remote-traps {
    categories remote-operations;
    targets {
      172.17.12.213;
    }
  }
}
```

For more information about trap groups, see [“Configuring SNMP Trap Groups” on page 1491](#).

Using Variable-Length String Indexes

All tabular objects in the remote operations MIBs supported by Junos OS are indexed by two variables of type **SnmpAdminString**. For more information about **SnmpAdminString**, see RFC 2571.

Junos OS does not handle **SnmpAdminString** any differently from the octet string variable type. However, the indexes are defined as variable length. When a variable length string is used as an index, the length of the string must be included as part of the object identifier (OID).

Example: Set Variable-Length String Indexes

To reference the **pingCtlTargetAddress** variable of a row in **pingCtlTable** where **pingCtlOwnerIndex** is **bob** and **pingCtlTestName** is **test**, use the following object identifier (OID):

```
pingMIB.pingObjects.pingCtlTable.pingCtlEntry.pingCtlTargetAddress."bob"."test"
1.3.6.1.2.1.80.1.2.1.4.3.98.111.98.4.116.101.115.116
```

For more information about the definition of the Ping MIB, see RFC 2925.

Enabling Logging

The SNMP error code returned in response to SNMP requests can only provide a generic description of the problem. The error descriptions logged by the remote operations process can often provide more detailed information about the problem and help you to solve the problem faster. This logging is not enabled by default. To enable logging, include the **flag general** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit]
snmp {
  traceoptions {
    flag general;
  }
}
```

For more information about traceoptions, see “Tracing SNMP Activity on a Device Running Junos OS” on page 1585.

If the remote operations process receives an SNMP request that it cannot accommodate, the error is logged in the **/var/log/rmopd** file. To monitor this log file, issue the **monitor start rmopd** command in operational mode of the command-line interface (CLI).

- Related Documentation**
- [Using the Ping MIB for Remote Monitoring Devices Running Junos OS on page 1562](#)
 - [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)

Using the Ping MIB for Remote Monitoring Devices Running Junos OS

A ping test is used to determine whether packets sent from the local host reach the designated host and are returned. If the designated host can be reached, the ping test provides the approximate round-trip time for the packets. Ping test results are stored in **pingResultsTable** and **pingProbeHistoryTable**.

RFC 2925 is the authoritative description of the Ping MIB in detail and provides the ASN.1 MIB definition of the Ping MIB.

- Related Documentation**
- [SNMP Remote Operations Overview on page 1559](#)
 - [Starting a Ping Test on page 1562](#)
 - [Monitoring a Running Ping Test on page 1564](#)
 - [Gathering Ping Test Results on page 1567](#)
 - [Stopping a Ping Test on page 1568](#)
 - [Interpreting Ping Variables on page 1568](#)

Starting a Ping Test

Before you start a ping test, configure a Ping MIB view. This allows SNMP **Set** requests on **pingMIB**. To start a ping test, create a row in **pingCtlTable** and set **pingCtlAdminStatus**

to **enabled**. The minimum information that must be specified before setting **pingCtlAdminStatus** to **enabled** is:

- **pingCtlOwnerIndexSnmpAdminString**
- **pingCtlTestNameSnmpAdminString**
- **pingCtlTargetAddressInetAddress**
- **pingCtlTargetAddressTypeInetAddressType**
- **pingCtlRowStatusRowStatus**

For all other values, defaults are chosen unless otherwise specified. **pingCtlOwnerIndex** and **pingCtlTestName** are used as the index, so their values are specified as part of the object identifier (OID). To create a row, set **pingCtlRowStatus** to **createAndWait** or **createAndGo** on a row that does not already exist. A value of **active** for **pingCtlRowStatus** indicates that all necessary information has been supplied and the test can begin; **pingCtlAdminStatus** can be set to **enabled**. An SNMP **Set** request that sets **pingCtlRowStatus** to **active** will fail if the necessary information in the row is not specified or is inconsistent. For information about how to configure a view, see [“Setting SNMP Views” on page 1560](#).

There are two ways to start a ping test:

- [Using Multiple Set Protocol Data Units \(PDUs\) on page 1563](#)
- [Using a Single Set PDU on page 1563](#)

Using Multiple Set Protocol Data Units (PDUs)

You can use multiple **Set** request PDUs (multiple PDUs, with one or more varbinds each) and set the following variables in this order to start the test:

- **pingCtlRowStatus** to **createAndWait**
- All appropriate test variables
- **pingCtlRowStatus** to **active**

Junos OS now verifies that all necessary information to run a test has been specified.

- **pingCtlAdminStatus** to **enabled**

Using a Single Set PDU

You can use a single **Set** request PDU (one PDU, with multiple varbinds) to set the following variables to start the test:

- **pingCtlRowStatus** to **createAndGo**
- All appropriate test variables
- **pingCtlAdminStatus** to **enabled**

Monitoring a Running Ping Test

When **pingCtlAdminStatus** is successfully set to **enabled**, the following is done before the acknowledgment of the SNMP **Set** request is sent back to the client:

- **pingResultsEntry** is created if it does not already exist.
- **pingResultsOperStatus** transitions to **enabled**.

For more information, see the following sections:

- [pingResultsTable on page 1564](#)
- [pingProbeHistoryTable on page 1565](#)
- [Generating Traps on page 1566](#)

pingResultsTable

While the test is running, **pingResultsEntry** keeps track of the status of the test. The value of **pingResultsOperStatus** is **enabled** while the test is running and **disabled** when it has stopped.

The value of **pingCtlAdminStatus** remains **enabled** until you set it to **disabled**. Thus, to get the status of the test, you must examine **pingResultsOperStatus**.

The **pingCtlFrequency** variable can be used to schedule many tests for one **pingCtlEntry**. After a test ends normally (you did not stop the test) and the **pingCtlFrequency** number of seconds has elapsed, the test is started again just as if you had set **pingCtlAdminStatus** to **enabled**. If you intervene at any time between repeated tests (you set **pingCtlAdminStatus** to **disabled** or **pingCtlRowStatus** to **notInService**), the repeat feature is disabled until another test is started and ends normally. A value of 0 for **pingCtlFrequency** indicates this repeat feature is not active.

pingResultsIpTgtAddr and **pingResultsIpTgtAddrType** are set to the value of the resolved destination address when the value of **pingCtlTargetAddressType** is **dns**. When a test starts successfully and **pingResultsOperStatus** transitions to **enabled**:

- **pingResultsIpTgtAddr** is set to **null-string**.
- **pingResultsIpTgtAddrType** is set to **unknown**.

pingResultsIpTgtAddr and **pingResultsIpTgtAddrType** are not set until **pingCtlTargetAddress** can be resolved to a numeric address. To retrieve these values, poll **pingResultsIpTgtAddrType** for any value other than **unknown** after successfully setting **pingCtlAdminStatus** to **enabled**.

At the start of a test, **pingResultsSentProbes** is initialized to 1 and the first probe is sent. **pingResultsSentProbes** increases by 1 each time a probe is sent.

As the test runs, every **pingCtlTimeOut** seconds, the following occur:

- **pingProbeHistoryStatus** for the corresponding **pingProbeHistoryEntry** in **pingProbeHistoryTable** is set to **requestTimedOut**.

- A **pingProbeFailed** trap is generated, if necessary.
- An attempt is made to send the next probe.



NOTE: No more than one outstanding probe exists for each test.

For every probe, you can receive one of the following results:

- The target host acknowledges the probe with a response.
- The probe times out; there is no response from the target host acknowledging the probe.
- The probe could not be sent.

Each probe result is recorded in **pingProbeHistoryTable**. For more information about **pingProbeHistoryTable**, see "[pingProbeHistoryTable](#)" on page 1565.

When a response is received from the target host acknowledging the current probe:

- **pingResultsProbeResponses** increases by 1.
- The following variables are updated:
 - **pingResultsMinRtt**—Minimum round-trip time
 - **pingResultsMaxRtt**—Maximum round-trip time
 - **pingResultsAverageRtt**—Average round-trip time
 - **pingResultsRttSumOfSquares**—Sum of squares of round-trip times
 - **pingResultsLastGoodProbe**—Timestamp of the last response



NOTE: Only probes that result in a response from the target host contribute to the calculation of the round-trip time (RTT) variables.

When a response to the last probe is received or the last probe has timed out, the test is complete.

pingProbeHistoryTable

An entry in **pingProbeHistoryTable** (**pingProbeHistoryEntry**) represents a probe result and is indexed by three variables:

- The first two variables, **pingCtlOwnerIndex** and **pingCtlTestName**, are the same ones used for **pingCtlTable**, which identifies the test.
- The third variable, **pingProbeHistoryIndex**, is a counter to uniquely identify each probe result.

The maximum number of **pingProbeHistoryTable** entries created for a given test is limited by **pingCtlMaxRows**. If **pingCtlMaxRows** is set to 0, no **pingProbeHistoryTable** entries are created for that test.

Each time a probe result is determined, a **pingProbeHistoryEntry** is created and added to **pingProbeHistoryTable**. **pingProbeHistoryIndex** of the new **pingProbeHistoryEntry** is 1 greater than the last **pingProbeHistoryEntry** added to **pingProbeHistoryTable** for that test. **pingProbeHistoryIndex** is set to 1 if this is the first entry in the table. The same test can be run multiple times, so this index keeps growing.

If **pingProbeHistoryIndex** of the last **pingProbeHistoryEntry** added is 0xFFFFFFFF, the next **pingProbeHistoryEntry** added has **pingProbeHistoryIndex** set to 1.

The following are recorded for each probe result:

- **pingProbeHistoryResponse**—Time to live (TTL)
- **pingProbeHistoryStatus**—What happened and why
- **pingProbeHistoryLastRC**—Return code (RC) value of ICMP packet
- **pingProbeHistoryTime**—Timestamp when probe result was determined

When a probe cannot be sent, **pingProbeHistoryResponse** is set to 0. When a probe times out, **pingProbeHistoryResponse** is set to the difference between the time when the probe was discovered to be timed out and the time when the probe was sent.

Generating Traps

For any trap to be generated, the appropriate bit of **pingCtlTrapGeneration** must be set. You must also configure a trap group to receive remote operations. A trap is generated under the following conditions:

- A **pingProbeFailed** trap is generated every time **pingCtlTrapProbeFailureFilter** number of consecutive probes fail during the test.
- A **pingTestFailed** trap is generated when the test completes and at least **pingCtlTrapTestFailureFilter** number of probes fail.
- A **pingTestCompleted** trap is generated when the test completes and fewer than **pingCtlTrapTestFailureFilter** probes fail.



NOTE: A probe is considered a failure when **pingProbeHistoryStatus** of the probe result is anything besides **responseReceived**.

For information about how to configure a trap group to receive remote operations, see [“Configuring SNMP Trap Groups” on page 1491](#) and [“Example: Setting Trap Notification for Remote Operations” on page 1561](#).

Gathering Ping Test Results

You can either poll **pingResultsOperStatus** to find out when the test is complete or request that a trap be sent when the test is complete. For more information about **pingResultsOperStatus**, see “[pingResultsTable](#)” on page 1564. For more information about Ping MIB traps, see “[Generating Traps](#)” on page 1566.

The statistics calculated and then stored in **pingResultsTable** include:

- **pingResultsMinRtt**—Minimum round-trip time
- **pingResultsMaxRtt**—Maximum round-trip time
- **pingResultsAverageRtt**—Average round-trip time
- **pingResultsProbeResponses**—Number of responses received
- **pingResultsSentProbes**—Number of attempts to send probes
- **pingResultsRttSumOfSquares**—Sum of squares of round-trip times
- **pingResultsLastGoodProbe**—Timestamp of the last response

You can also consult **pingProbeHistoryTable** for more detailed information about each probe. The index used for **pingProbeHistoryTable** starts at 1, goes to 0xFFFFFFFF, and wraps to 1 again.

For example, if **pingCtlProbeCount** is 15 and **pingCtlMaxRows** is 5, then upon completion of the first run of this test, **pingProbeHistoryTable** contains probes like those in [Table 119](#).

Table 119: Results in pingProbeHistoryTable: After the First Ping Test

pingProbeHistoryIndex	Probe Result
11	Result of 11th probe from run 1
12	Result of 12th probe from run 1
13	Result of 13th probe from run 1
14	Result of 14th probe from run 1
15	Result of 15th probe from run 1

Upon completion of the first probe of the second run of this test, **pingProbeHistoryTable** will contain probes like those in [Table 120](#).

Table 120: Results in pingProbeHistoryTable: After the First Probe of the Second Test

pingProbeHistoryIndex	Probe Result
12	Result of 12th probe from run 1

Table 120: Results in pingProbeHistoryTable: After the First Probe of the Second Test (*continued*)

pingProbeHistoryIndex	Probe Result
13	Result of 13th probe from run 1
14	Result of 14th probe from run 1
15	Result of 15th probe from run 1
16	Result of 1st probe from run 2

Upon completion of the second run of this test, **pingProbeHistoryTable** will contain probes like those in [Table 121](#).

Table 121: Results in pingProbeHistoryTable: After the Second Ping Test

pingProbeHistoryIndex	Probe Result
26	Result of 11th probe from run 2
27	Result of 12th probe from run 2
28	Result of 13th probe from run 2
29	Result of 14th probe from run 2
30	Result of 15th probe from run 2

History entries can be deleted from the MIB in two ways:

- More history entries for a given test are added and the number of history entries exceeds **pingCtlMaxRows**. The oldest history entries are deleted to make room for the new ones.
- You delete the entire test by setting **pingCtlRowStatus** to **destroy**.

Stopping a Ping Test

To stop an active test, set **pingCtlAdminStatus** to **disabled**. To stop the test and remove its **pingCtlEntry**, **pingResultsEntry**, and any **pingHistoryEntry** objects from the MIB, set **pingCtlRowStatus** to **destroy**.

Interpreting Ping Variables

This section clarifies the ranges for the following variables that are not explicitly specified in the Ping MIB:

- **pingCtlDataSize**—The value of this variable represents the total size of the payload (in bytes) of an outgoing probe packet. This payload includes the timestamp (8 bytes) that is used to time the probe. This is consistent with the definition of **pingCtlDataSize** (maximum value of 65,507) and the standard ping application.

If the value of **pingCtlDataSize** is between 0 and 8 inclusive, it is ignored and the payload is 8 bytes (the timestamp). The Ping MIB assumes all probes are timed, so the payload must always include the timestamp.

For example, if you wish to add an additional 4 bytes of payload to the packet, you must set **pingCtlDataSize** to 12.

- **pingCtlDataFill**—The first 8 bytes of the data segment of the packet is for the timestamp. After that, the **pingCtlDataFill** pattern is used in repetition. The default pattern (when **pingCtlDataFill** is not specified) is (00, 01, 02, 03 ... FF, 00, 01, 02, 03 ... FF, ...).
- **pingCtlMaxRows**—The maximum value is 255.
- **pingMaxConcurrentRequests**—The maximum value is 500.
- **pingCtlTrapProbeFailureFilter** and **pingCtlTrapTestFailureFilter**—A value of 0 for **pingCtlTrapProbeFailureFilter** or **pingCtlTrapTestFailureFilter** is not well defined by the Ping MIB. If **pingCtlTrapProbeFailureFilter** is 0, **pingProbeFailed** traps will not be generated for the test under any circumstances. If **pingCtlTrapTestFailureFilter** is 0, **pingTestFailed** traps will not be generated for the test under any circumstances.

Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS

A traceroute test approximates the path packets take from the local host to the remote host.

RFC 2925 is the authoritative description of the Traceroute MIB in detail and provides the ASN.1 MIB definition of the Traceroute MIB.

Related Documentation

- [SNMP Remote Operations Overview on page 1559](#)
- [Starting a Traceroute Test on page 1570](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Stopping a Traceroute Test on page 1577](#)
- [Interpreting Traceroute Variables on page 1578](#)

Starting a Traceroute Test

Before you start a traceroute test, configure a Traceroute MIB view. This allows SNMP **Set** requests on **tracerouteMIB**. To start a test, create a row in **traceRouteCtlTable** and set **traceRouteCtlAdminStatus** to **enabled**. You must specify at least the following before setting **traceRouteCtlAdminStatus** to **enabled**:

- **traceRouteCtlOwnerIndexSnmpAdminString**
- **traceRouteCtlTestNameSnmpAdminString**
- **traceRouteCtlTargetAddressInetAddress**
- **traceRouteCtlRowStatusRowStatus**

For all other values, defaults are chosen unless otherwise specified.

traceRouteCtlOwnerIndex and **traceRouteCtlTestName** are used as the index, so their values are specified as part of the OID. To create a row, set **traceRouteCtlRowStatus** to **createAndWait** or **createAndGo** on a row that does not already exist. A value of **active** for **traceRouteCtlRowStatus** indicates that all necessary information has been specified and the test can begin; **traceRouteCtlAdminStatus** can be set to **enabled**. An SNMP **Set** request that sets **traceRouteCtlRowStatus** to **active** will fail if the necessary information in the row is not specified or is inconsistent. For information about how to configure a view, see [“Setting SNMP Views” on page 1560](#).

There are two ways to start a traceroute test:

- [Using Multiple Set PDUs on page 1570](#)
- [Using a Single Set PDU on page 1570](#)

Using Multiple Set PDUs

You can use multiple **Set** request PDUs (multiple PDUs, with one or more varbinds each) and set the following variables in this order to start the test:

- **traceRouteCtlRowStatus** to **createAndWait**
- All appropriate test variables
- **traceRouteCtlRowStatus** to **active**

The Junos OS now verifies that all necessary information to run a test has been specified.

- **traceRouteCtlAdminStatus** to **enabled**

Using a Single Set PDU

You can use a single **Set** request PDU (one PDU, with multiple varbinds) to set the following variables to start the test:

- **traceRouteCtlRowStatus** to **createAndGo**
- All appropriate test variables

- **traceRouteCtlAdminStatus** to enabled

Related Documentation

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [SNMP Remote Operations Overview on page 1559](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Stopping a Traceroute Test on page 1577](#)
- [Interpreting Traceroute Variables on page 1578](#)

Monitoring a Running Traceroute Test

When **traceRouteCtlAdminStatus** is successfully set to **enabled**, the following is done before the acknowledgment of the SNMP **Set** request is sent back to the client:

- **traceRouteResultsEntry** is created if it does not already exist.
- **traceRouteResultsOperStatus** transitions to enabled.

For more information, see the following sections:

- [traceRouteResultsTable on page 1571](#)
- [traceRouteProbeResultsTable on page 1572](#)
- [traceRouteHopsTable on page 1573](#)
- [Generating Traps on page 1574](#)

traceRouteResultsTable

While the test is running, this **traceRouteResultsTable** keeps track of the status of the test. The value of **traceRouteResultsOperStatus** is **enabled** while the test is running and **disabled** when it has stopped.

The value of **traceRouteCtlAdminStatus** remains **enabled** until you set it to **disabled**. Thus, to get the status of the test, you must examine **traceRouteResultsOperStatus**.

The **traceRouteCtlFrequency** variable can be used to schedule many tests for one **traceRouteCtlEntry**. After a test ends normally (you did not stop the test) and **traceRouteCtlFrequency** number of seconds has elapsed, the test is started again just as if you had set **traceRouteCtlAdminStatus** to **enabled**. If you intervene at any time between repeated tests (you set **traceRouteCtlAdminStatus** to **disabled** or **traceRouteCtlRowStatus** to **notInService**), the repeat feature is **disabled** until another test is started and ends normally. A value of 0 for **traceRouteCtlFrequency** indicates this repeat feature is not active.

traceRouteResultsIpTgtAddr and **traceRouteResultsIpTgtAddrType** are set to the value of the resolved destination address when the value of **traceRouteCtlTargetAddressType**

is **dns**. When a test starts successfully and **traceRouteResultsOperStatus** transitions to **enabled**:

- **traceRouteResultsIpTgtAddr** is set to null-string.
- **traceRouteResultsIpTgtAddrType** is set to unknown.

traceRouteResultsIpTgtAddr and **traceRouteResultsIpTgtAddrType** are not set until **traceRouteCtlTargetAddress** can be resolved to a numeric address. To retrieve these values, poll **traceRouteResultsIpTgtAddrType** for any value other than **unknown** after successfully setting **traceRouteCtlAdminStatus** to **enabled**.

At the start of a test, **traceRouteResultsCurHopCount** is initialized to **traceRouteCtlInitialTtl**, and **traceRouteResultsCurProbeCount** is initialized to 1. Each time a probe result is determined, **traceRouteResultsCurProbeCount** increases by 1. While the test is running, the value of **traceRouteResultsCurProbeCount** reflects the current outstanding probe for which results have not yet been determined.

The **traceRouteCtlProbesPerHop** number of probes is sent for each time-to-live (TTL) value. When the result of the last probe for the current hop is determined, provided that the current hop is not the destination hop, **traceRouteResultsCurHopCount** increases by 1, and **traceRouteResultsCurProbeCount** resets to 1.

At the start of a test, if this is the first time this test has been run for this **traceRouteCtlEntry**, **traceRouteResultsTestAttempts** and **traceRouteResultsTestSuccesses** are initialized to 0.

At the end of each test execution, **traceRouteResultsOperStatus** transitions to **disabled**, and **traceRouteResultsTestAttempts** increases by 1. If the test was successful in determining the full path to the target, **traceRouteResultsTestSuccesses** increases by 1, and **traceRouteResultsLastGoodPath** is set to the current time.

traceRouteProbeResultsTable

Each entry in **traceRouteProbeHistoryTable** is indexed by five variables:

- The first two variables, **traceRouteCtlOwnerIndex** and **traceRouteCtlTestName**, are the same ones used for **traceRouteCtlTable** and to identify the test.
- The third variable, **traceRouteProbeHistoryIndex**, is a counter, starting from 1 and wrapping at FFFFFFFF. The maximum number of entries is limited by **traceRouteCtlMaxRows**.
- The fourth variable, **traceRouteProbeHistoryHopIndex**, indicates which hop this probe is for (the actual time-to-live or TTL value). Thus, the first **traceRouteCtlProbesPerHop** number of entries created when a test starts have a value of **traceRouteCtlInitialTtl** for **traceRouteProbeHistoryHopIndex**.
- The fifth variable, **traceRouteProbeHistoryProbeIndex**, is the probe for the current hop. It ranges from 1 to **traceRouteCtlProbesPerHop**.

While a test is running, as soon as a probe result is determined, the next probe is sent. A maximum of **traceRouteCtlTimeOut** seconds elapses before a probe is marked with

status **requestTimedOut** and the next probe is sent. There is never more than one outstanding probe per traceroute test. Any probe result coming back after a probe times out is ignored.

Each probe can:

- Result in a response from a host acknowledging the probe
- Time out with no response from a host acknowledging the probe
- Fail to be sent

Each probe status is recorded in **traceRouteProbeHistoryTable** with **traceRouteProbeHistoryStatus** set accordingly.

Probes that result in a response from a host record the following data:

- **traceRouteProbeHistoryResponse**—Round-trip time (RTT)
- **traceRouteProbeHistoryHAddrType**—The type of HAddr (next argument)
- **traceRouteProbeHistoryHAddr**—The address of the hop

All probes, regardless of whether a response for the probe is received, have the following recorded:

- **traceRouteProbeHistoryStatus**—What happened and why
- **traceRouteProbeHistoryLastRC**—Return code (RC) value of the ICMP packet
- **traceRouteProbeHistoryTime**—Timestamp when the probe result was determined

When a probe cannot be sent, **traceRouteProbeHistoryResponse** is set to 0. When a probe times out, **traceRouteProbeHistoryResponse** is set to the difference between the time when the probe was discovered to be timed out and the time when the probe was sent.

traceRouteHopsTable

Entries in **traceRouteHopsTable** are indexed by three variables:

- The first two, **traceRouteCtlOwnerIndex** and **traceRouteCtlTestName**, are the same ones used for **traceRouteCtlTable** and identify the test.
- The third variable, **traceRouteHopsHopIndex**, indicates the current hop, which starts at 1 (not **traceRouteCtlInitialTtl**).

When a test starts, all entries in **traceRouteHopsTable** with the given **traceRouteCtlOwnerIndex** and **traceRouteCtlTestName** are deleted. Entries in this table are only created if **traceRouteCtlCreateHopsEntries** is set to **true**.

A new **traceRouteHopsEntry** is created each time the first probe result for a given TTL is determined. The new entry is created whether or not the first probe reaches a host. The value of **traceRouteHopsHopIndex** is increased by 1 for this new entry.



NOTE: Any `traceRouteHopsEntry` can lack a value for `traceRouteHopsIpTgtAddress` if there are no responses to the probes with the given TTL.

Each time a probe reaches a host, the IP address of that host is available in the probe result. If the value of `traceRouteHopsIpTgtAddress` of the current `traceRouteHopsEntry` is not set, then the value of `traceRouteHopsIpTgtAddress` is set to this IP address. If the value of `traceRouteHopsIpTgtAddress` of the current `traceRouteHopsEntry` is the same as the IP address, then the value does not change. If the value of `traceRouteHopsIpTgtAddress` of the current `traceRouteHopsEntry` is different from this IP address, indicating a path change, a new `traceRouteHopsEntry` is created with:

- `traceRouteHopsHopIndex` variable increased by 1
- `traceRouteHopsIpTgtAddress` set to the IP address



NOTE: A new entry for a test is added to `traceRouteHopsTable` each time a new TTL value is used or the path changes. Thus, the number of entries for a test may exceed the number of different TTL values used.

When a probe result is determined, the value `traceRouteHopsSentProbes` of the current `traceRouteHopsEntry` increases by 1. When a probe result is determined, and the probe reaches a host:

- The value `traceRouteHopsProbeResponses` of the current `traceRouteHopsEntry` is increased by 1.
- The following variables are updated:
 - `traceRouteResultsMinRtt`—Minimum round-trip time
 - `traceRouteResultsMaxRtt`—Maximum round-trip time
 - `traceRouteResultsAverageRtt`—Average round-trip time
 - `traceRouteResultsRttSumOfSquares`—Sum of squares of round-trip times
 - `traceRouteResultsLastGoodProbe`—Timestamp of the last response



NOTE: Only probes that reach a host affect the round-trip time values.

Generating Traps

For any trap to be generated, the appropriate bit of `traceRouteCtlTrapGeneration` must be set. You must also configure a trap group to receive remote operations. Traps are generated under the following conditions:

- **traceRouteHopsIpTgtAddress** of the current probe is different from the last probe with the same TTL value (**traceRoutePathChange**).
- A path to the target could not be determined (**traceRouteTestFailed**).

A path to the target was determined (**traceRouteTestCompleted**).

For information about how to configure a trap group to receive remote operations, see [“Configuring SNMP Trap Groups” on page 1491](#) and [“Example: Setting Trap Notification for Remote Operations” on page 1561](#).

Monitoring Traceroute Test Completion

When a test is complete, **traceRouteResultsOperStatus** transitions from **enabled** to **disabled**. This transition occurs in the following situations:

- The test ends successfully. A probe result indicates that the destination has been reached. In this case, the current hop is the last hop. The rest of the probes for this hop are sent. When the last probe result for the current hop is determined, the test ends.
- **traceRouteCtlMaxTtl** threshold is exceeded. The destination is never reached. The test ends after the number of probes with TTL value equal to **traceRouteCtlMaxttl** have been sent.
- **traceRouteCtlMaxFailures** threshold is exceeded. The number of consecutive probes that end with status **requestTimedOut** exceeds **traceRouteCtlMaxFailures**.
- You end the test. You set **traceRouteCtlAdminStatus** to **disabled** or delete the row by setting **traceRouteCtlRowStatus** to **destroy**.
- You misconfigured the traceroute test. A value or variable you specified in **traceRouteCtlTable** is incorrect and will not allow a single probe to be sent. Because of the nature of the data, this error could not be determined until the test was started; that is, until after **traceRouteResultsOperStatus** transitioned to **enabled**. When this occurs, one entry is added to **traceRouteProbeHistoryTable** with **traceRouteProbeHistoryStatus** set to the appropriate error code.

If **traceRouteCtlTrapGeneration** is set properly, either the **traceRouteTestFailed** or **traceRouteTestCompleted** trap is generated.

Related Documentation

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [SNMP Remote Operations Overview on page 1559](#)
- [Starting a Traceroute Test on page 1570](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Stopping a Traceroute Test on page 1577](#)
- [Interpreting Traceroute Variables on page 1578](#)

Gathering Traceroute Test Results

You can either poll **traceRouteResultsOperStatus** to find out when the test is complete or request that a trap be sent when the test is complete. For more information about **traceResultsOperStatus**, see [“traceRouteResultsTable” on page 1571](#). For more information about Traceroute MIB traps, see the Generating Traps section in [“Monitoring a Running Traceroute Test” on page 1571](#).

Statistics are calculated on a per-hop basis and then stored in **traceRouteHopsTable**. They include the following for each hop:

- **traceRouteHopsIpTgtAddressType**—Address type of host at this hop
- **traceRouteHopsIpTgtAddress**—Address of host at this hop
- **traceRouteHopsMinRtt**—Minimum round-trip time
- **traceRouteHopsMaxRtt**—Maximum round-trip time
- **traceRouteHopsAverageRtt**—Average round-trip time
- **traceRouteHopsRttSumOfSquares**—Sum of squares of round-trip times
- **traceRouteHopsSentProbes**—Number of attempts to send probes
- **traceRouteHopsProbeResponses**—Number of responses received
- **traceRouteHopsLastGoodProbe**—Timestamp of last response

You can also consult **traceRouteProbeHistoryTable** for more detailed information about each probe. The index used for **traceRouteProbeHistoryTable** starts at 1, goes to 0xFFFFFFFF, and wraps to 1 again.

For example, assume the following:

- **traceRouteCtlMaxRows** is 10.
- **traceRouteCtlProbesPerHop** is 5.
- There are eight hops to the target (the target being number eight).
- Each probe sent results in a response from a host (the number of probes sent is not limited by **traceRouteCtlMaxFailures**).

In this test, 40 probes are sent. At the end of the test, **traceRouteProbeHistoryTable** would have a history of probes like those in [Table 122](#).

Table 122: traceRouteProbeHistoryTable

HistoryIndex	HistoryHopIndex	HistoryProbeIndex
31	7	1
32	7	2
33	7	3

Table 122: traceRouteProbeHistoryTable (*continued*)

HistoryIndex	HistoryHopIndex	HistoryProbeIndex
34	7	4
35	7	5
36	8	1
37	8	2
38	8	3
39	8	4
40	8	5

Related Documentation

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [SNMP Remote Operations Overview on page 1559](#)
- [Starting a Traceroute Test on page 1570](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Stopping a Traceroute Test on page 1577](#)
- [Interpreting Traceroute Variables on page 1578](#)

Stopping a Traceroute Test

To stop an active test, set **traceRouteCtlAdminStatus** to **disabled**. To stop a test and remove its **traceRouteCtlEntry**, **traceRouteResultsEntry**, **traceRouteProbeHistoryEntry**, and **traceRouteProbeHistoryEntry** objects from the MIB, set **traceRouteCtlRowStatus** to **destroy**.

Related Documentation

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [SNMP Remote Operations Overview on page 1559](#)
- [Starting a Traceroute Test on page 1570](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Interpreting Traceroute Variables on page 1578](#)

Interpreting Traceroute Variables

This topic contains information about the ranges for the following variables that are not explicitly specified in the Traceroute MIB:

- **traceRouteCtlMaxRows**—The maximum value for **traceRouteCtlMaxRows** is 2550. This represents the maximum TTL (255) multiplied by the maximum for **traceRouteCtlProbesPerHop** (10). Therefore, the **traceRouteProbeHistoryTable** accommodates one complete test at the maximum values for one **traceRouteCtlEntry**. Usually, the maximum values are not used and the **traceRouteProbeHistoryTable** is able to accommodate the complete history for many tests for the same **traceRouteCtlEntry**.
- **traceRouteMaxConcurrentRequests**—The maximum value is 50. If a test is running, it has one outstanding probe. **traceRouteMaxConcurrentRequests** represents the maximum number of traceroute tests that have **traceRouteResultsOperStatus** with a value of **enabled**. Any attempt to start a test with **traceRouteMaxConcurrentRequests** tests running will result in the creation of one probe with **traceRouteProbeHistoryStatus** set to **maxConcurrentLimitReached** and that test will end immediately.
- **traceRouteCtlTable**—The maximum number of entries allowed in this table is 100. Any attempt to create a 101st entry will result in a **BAD_VALUE** message for SNMPv1 and a **RESOURCE_UNAVAILABLE** message for SNMPv2.

Related Documentation

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1569](#)
- [Monitoring a Running Traceroute Test on page 1571](#)
- [SNMP Remote Operations Overview on page 1559](#)
- [Starting a Traceroute Test on page 1570](#)
- [Monitoring Traceroute Test Completion on page 1575](#)
- [Gathering Traceroute Test Results on page 1576](#)
- [Stopping a Traceroute Test on page 1577](#)

CHAPTER 67

Tracing SNMP Activity

- [Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS on page 1579](#)
- [Tracing SNMP Activity on a Device Running Junos OS on page 1585](#)
- [Example: Tracing SNMP Activity on page 1588](#)

Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS

The following sections contain information about monitoring the SNMP activity on devices running the Junos OS and identifying problems that might impact the SNMP performance on devices running Junos OS:

- [Checking for MIB Objects Registered with the snmpd on page 1579](#)
- [Tracking SNMP Activity on page 1580](#)
- [Monitoring SNMP Statistics on page 1582](#)
- [Checking CPU Utilization on page 1583](#)
- [Checking Kernel and Packet Forwarding Engine Response on page 1584](#)

Checking for MIB Objects Registered with the snmpd

For the SNMP process to be able to access data related to a MIB object, the MIB object must be registered with the snmpd. When an SNMP subagent comes online, it tries to register the associated MIB objects with the snmpd. The snmpd maintains a mapping of the objects and the subagents with which the objects are associated. However, the registration attempt fails occasionally, and the objects remain unregistered with the snmpd until the next time the subagent restarts and successfully registers the objects.

When a network management system polls for data related to objects that are not registered with the snmpd, the snmpd returns either a **noSuchName** error (for SNMPv1 objects) or a **noSuchObject** error (for SNMPv2 objects).

You can use the following commands to check for MIB objects that are registered with the snmpd:

- **show snmp registered-objects**—Creates a `/var/log/snmp_reg_objs` file that contains the list of registered objects and their mapping to various subagents.

- **file show /var/log/snmp_reg_objs**—Displays the contents of the `/var/log/snmp_reg_objs` file.

The following example shows the steps for creating and displaying the `/var/log/snmp_reg_objs` file:

```
user@host> show snmp registered-objects
user@host> file show /var/log/snmp_reg_objs

-----
Registered MIB Objects
root_name =
-----
.1.2.840.10006.300.43.1.1.1.1.2 (dot3adAggMACAddress) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.3 (dot3adAggActorSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.4 (dot3adAggActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.5 (dot3adAggAggregateOrIndividual)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.6 (dot3adAggActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.7 (dot3adAggActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.8 (dot3adAggPartnerSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.9 (dot3adAggPartnerSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.10 (dot3adAggPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.11 (dot3adAggCollectorMaxDelay) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.2.1.1 (dot3adAggPortListPorts) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.2 (dot3adAggPortActorSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.3 (dot3adAggPortActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.4 (dot3adAggPortActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.5 (dot3adAggPortActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.6 (dot3adAggPortPartnerAdminSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.7 (dot3adAggPortPartnerOperSystemPriority)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.8 (dot3adAggPortPartnerAdminSystemID)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.9 (dot3adAggPortPartnerOperSystemID)
(/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.10 (dot3adAggPortPartnerAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.11 (dot3adAggPortPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.12 (dot3adAggPortSelectedAggID) (/var/run/mib2d-11)
---(more)---
```



NOTE: The `/var/log/snmp_reg_objs` file contains only those objects that are associated with the Junos OS processes that are up and running and registered with the `snmpd`, at the time of executing the `show snmp registered-objects` command. If a MIB object related to a Junos OS process that is up and running is not shown in the list of registered objects, you might want to restart the software process to retry object registration with the `snmpd`.

Tracking SNMP Activity

SNMP tracing operations track activity of SNMP agents and record the information in log files. The logged event descriptions provide detailed information to help you solve problems faster. By default, Junos OS does not trace any SNMP activity. To enable

A sample `traceoptions` configuration might look like:

When the **traceoptions** flag all statement is included at the **[edit snmp]** hierarchy level, the following log files are created:

- You can use the **show log log-filename** operational mode command to view the contents of the log file. In the snmpd log file (see the following example), a sequence of >>> represents an incoming packet, whereas a sequence of <<< represents an outgoing packet. Note that the request response pair might not follow any sequence if there are multiple network management systems polling the device at the same time. You can use the source and request ID combinations to match requests and responses. However, note that no response log is created in the log file if the SNMP master agent or the SNMP subagent has not responded to a request.

Reviewing a Log File

[illegible]

[illegible]

Monitoring SNMP Statistics

The **show snmp statistics extensive** operational mode command provides you with an option to review SNMP traffic, including traps, on a device. Output for the **show snmp statistics extensive** command shows real-time values and can be used to monitor values such as throttle drops, currently active, max active, not found, time out, max latency, current queued, total queued, and overflows. You can identify slowness in SNMP responses by monitoring the currently active count, because a constant increase in the currently active count is directly linked to slow or no response to SNMP requests.

Sample Output for the show snmp statistics extensive Command

```

user@host> show snmp statistics extensive
SNMP statistics:
Input:
  Packets: 226656, Bad versions: 0, Bad community names: 0,
  Bad community uses: 0, ASN parse errors: 0,
  Too big: 0, No such names: 0, Bad values: 0,
  Read only: 0, General errors: 0,
  Total request varbinds: 1967606, Total set varbinds: 0,
  Get requests: 18478, Get nexts: 75794, Set requests: 0,
  Get responses: 0, Traps: 0,
  Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
  Throttle drops: 27084, Duplicate request drops: 0
V3 Input:
  Unknown security models: 0, Invalid messages: 0
  Unknown pdu handlers: 0, Unavailable contexts: 0
  Unknown contexts: 0, Unsupported security levels: 0
  Not in time windows: 0, Unknown user names: 0
  Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
Output:
  Packets: 226537, Too big: 0, No such names: 0,
  Bad values: 0, General errors: 0,
  Get requests: 0, Get nexts: 0, Set requests: 0,
  Get responses: 226155, Traps: 382
SA Control Blocks:
  Total: 222984, Currently Active: 501, Max Active: 501,
  Not found: 0, Timed Out: 0, Max Latency: 25
SA Registration:
  Registers: 0, Deregisters: 0, Removes: 0
Trap Queue Stats:
  Current queued: 0, Total queued: 0, Discards: 0, Overflows: 0
Trap Throttle Stats:
  Current throttled: 0, Throttles needed: 0
Snmp Set Stats:
  Commit pending failures: 0, Config lock failures: 0
  Rpc failures: 0, Journal write failures: 0
  Mgd connect failures: 0, General commit failures: 0

```

Checking CPU Utilization

High CPU usage of the software processes that are being queried, such as `snmpd` or `mib2d`, is another factor that can lead to slow response or no response. You can use the **show system processes extensive** operational mode command to check the CPU usage levels of the Junos OS processes.

Sample Output of show system processes extensive Command

```

user@host> show system processes extensive
last pid: 1415; load averages: 0.00, 0.00, 0.00 up 0+02:20:54 10:26:25
117 processes: 2 running, 98 sleeping, 17 waiting

Mem: 180M Active, 54M Inact, 39M Wired, 195M Cache, 69M Buf, 272M Free
Swap: 1536M Total, 1536M Free

```

PID	USERNAME	THR	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	COMMAND
11	root	1	171	52	OK	12K	RUN	132:09	95.21%	idle
1184	root	1	97	0	35580K	9324K	select	4:16	1.61%	chassisd
177	root	1	-8	0	OK	12K	mdwait	0:51	0.00%	md7

```

119 root      1  -8    0    OK    12K mdwait  0:20  0.00% md4
13 root      1 -20 -139    OK    12K WAIT    0:16  0.00% swi7: clock sio
1373 root     1 96    0 15008K 12712K select 0:09  0.00% snmpd
1371 root     1 96    0 9520K  5032K select 0:08  0.00% jdiameterd
12 root      1 -40 -159    OK    12K WAIT    0:07  0.00% swi2: net
1375 root     2 96    0 15016K 5812K select 0:06  0.00% pfed
49 root      1  -8    0    OK    12K mdwait  0:05  0.00% md0
1345 root     1 96    0 10088K 4480K select 0:05  0.00% l2ald
1181 root     1 96    0 1608K  908K select 0:05  0.00% bslockd
23 root      1 -68 -187    OK    12K WAIT    0:04  0.00% irq10: fxp1
30 root      1 171  52    OK    12K pgzero   0:04  0.00% pagezero
1344 root     1  4    0 39704K 11444K kqread 0:03  0.00% rpd
1205 root     1 96    0 3152K  912K select 0:03  0.00% license-check
1372 root     1 96    0 28364K 6696K select 0:03  0.00% dcd
1374 root     1 96    0 11764K 7632K select 0:02  0.00% mib2d
1405 user     1 96    0 15892K 11132K select 0:02  0.00% cli
139 root      1  -8    0    OK    12K mdwait  0:02  0.00% md5
22 root      1 -80 -199    OK    12K WAIT    0:02  0.00% irq9: cbb1 fxp0
1185 root     1 96    0 4472K  2036K select 0:02  0.00% alarmd
4 root       1  -8    0    OK    12K -        0:02  0.00% g_down
3 root       1  -8    0    OK    12K -        0:02  0.00% g_up
43 root      1 -16    0    OK    12K psleep   0:02  0.00% vmkmemdaemon
1377 root     1 96    0 3776K  2256K select 0:01  0.00% irsd
48 root      1 -16    0    OK    12K -        0:01  0.00% schedcpu
99 root      1  -8    0    OK    12K mdwait  0:01  0.00% md3
953 root     1 96    0 4168K  2428K select 0:01  0.00% eventd
1364 root     1 96    0 4872K  2808K select 0:01  0.00% cfmd
15 root      1 -16    0    OK    12K -        0:01  0.00% yarrow
1350 root     1 96    0 31580K 7248K select 0:01  0.00% cosd
1378 root     1 96    0 19776K 6292K select 0:01  0.00% lpdfd

```

...

Checking Kernel and Packet Forwarding Engine Response

As mentioned in [“Understanding SNMP Implementation in Junos OS” on page 1403](#), some SNMP MIB data are maintained by the kernel or Packet Forwarding Engine. For such data to be available for the network management system, the kernel has to provide the required information to the SNMP subagent in mib2d. A slow response from the kernel can cause a delay in mib2d returning the data to the network management system. Junos OS adds an entry in the mib2d log file every time that an interface takes more than 10,000 microseconds to respond to a request for interface statistics. You can use the **show log log-filename | grep “kernel response time”** command to find out the response time taken by the kernel.

Checking the Kernel Response Time

```

user@host> show log mib2d | grep “kernel response time”
Aug 17 22:39:37 == kernel response time for
COS_IPVPN_DEFAULT_OUTPUT-t1-7/3/0:10:27.0-o: 9.126471 sec, range
(0.000007, 11.000806)

Aug 17 22:39:53 == kernel response time for
COS_IPVPN_DEFAULT_INPUT-t1-7/2/0:5:15.0-i: 5.387321 sec, range
(0.000007, 11.000806)

Aug 17 22:39:53 == kernel response time for ct1-6/1/0:9:15: 0.695406
sec, range (0.000007, 11.000806)

```


Aug 17 22:40:04 == kernel response time for t1-6/3/0:6:19: 1.878542 sec, range (0.000007, 11.000806)

Aug 17 22:40:22 == kernel response time for lsq-7/0/0: 2.556592 sec, range (0.000007, 11.000806)

Related Documentation

- [Understanding SNMP Implementation in Junos OS on page 1403](#)
- [Configuring SNMP on Devices Running Junos OS on page 1471](#)
- [Optimizing the Network Management System Configuration for the Best Results on page 1467](#)
- [Configuring Options on Managed Devices for Better SNMP Response Time on page 1469](#)
- *Managing Traps and Informs*
- *Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage*

Tracing SNMP Activity on a Device Running Junos OS

SNMP tracing operations track activity for SNMP agents and record the information in log files. The logged error descriptions provide detailed information to help you solve problems faster.

By default, Junos OS does not trace any SNMP activity. If you include the **traceoptions** statement at the **[edit snmp]** hierarchy level, the default tracing behavior is:

- Important activities are logged in files located in the **/var/log** directory. Each log is named after the SNMP agent that generates it. Currently, the following log files are created in the **/var/log** directory when the **traceoptions** statement is used:
 - chassisd
 - craftd
 - ilmid
 - mib2d
 - rmopd
 - serviced
 - snmpd
- When a trace file named **filename** reaches its maximum size, it is renamed **filename.0**, then **filename.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. (For more information about how log files are created, see the [System Log Explorer](#).)
- Log files can be accessed only by the user who configured the tracing operation.

You cannot change the directory (`/var/log`) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the `[edit snmp]` hierarchy level:

```
[edit snmp]
traceoptions {
  file <files number> <match regular-expression> <size size> <world-readable |
    no-world-readable>;
  flag flag;
  memory-trace;
  no-remote-trace;
  no-default-memory-trace;
}
```

These statements are described in the following sections:

- [Configuring the Number and Size of SNMP Log Files on page 1586](#)
- [Configuring Access to the Log File on page 1586](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 1587](#)
- [Configuring the Trace Operations on page 1587](#)

Configuring the Number and Size of SNMP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename.0*, then *filename.1*, and so on, until there are three trace files. Then the oldest trace file (*filename.2*) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the `[edit snmp traceoptions]` hierarchy level:

```
[edit snmp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename.0*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0* is renamed *filename.1* and *filename* is renamed *filename.0*. This process repeats until there are 20 trace files. Then the oldest file (*filename.19*) is overwritten by the newest file (*filename.0*).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configured the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the `[edit snmp traceoptions]` hierarchy level:

```
[edit snmp traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged activities.

You can refine the output by including the **match** statement at the **[edit snmp traceoptions file filename]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit snmp traceoptions]
file filename match regular-expression;
```

Configuring the Trace Operations

By default, only important activities are logged. You can specify which trace operations are to be logged by including the following **flag** statement (with one or more tracing flags) at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
flag {
  all;
  configuration;
  database;
  events;
  general;
  interface-stats;
  nonvolatile-sets;
  pdu;
  policy;
  protocol-timeouts;
  routing-socket;
  server;
  subagent;
  timer;
  varbind-error;
}
```

Table 123 describes the meaning of the SNMP tracing flags.

Table 123: SNMP Tracing Flags

Flag	Description	Default Setting
all	Log all operations.	Off
configuration	Log reading of the configuration at the [edit snmp] hierarchy level.	Off
database	Log events involving storage and retrieval in the events database.	Off
events	Log important events.	Off

Table 123: SNMP Tracing Flags (*continued*)

Flag	Description	Default Setting
general	Log general events.	Off
interface-stats	Log physical and logical interface statistics.	Off
nonvolatile-set	Log nonvolatile SNMP set request handling.	Off
pdu	Log SNMP request and response packets.	Off
policy	Log policy processing.	Off
protocol-timeouts	Log SNMP response timeouts.	Off
routing-socket	Log routing socket calls.	Off
server	Log communication with processes that are generating events.	Off
subagent	Log subagent restarts.	Off
timer	Log internal timer events.	Off
varbind-error	Log variable binding errors.	Off

To display the end of the log for an agent, issue the **show log agentd | last** operational mode command:

```
[edit]
user@host# run show log agentd | last
```

where **agent** is the name of an SNMP agent.

Related Documentation

- [Configuring SNMP on a Device Running Junos OS](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)
- [Example: Tracing SNMP Activity on page 1588](#)
- [Configuring SNMP](#)

Example: Tracing SNMP Activity

Trace information about SNMP packets:

```
[edit]
snmp {
  traceoptions {
    file size 10k files 5;
    flag pdu;
    flag protocol-timeouts;
```

```
        flag varbind-error;  
    }  
}
```

**Related
Documentation**

- *Configuring SNMP on a Device Running Junos OS*
- [Tracing SNMP Activity on a Device Running Junos OS on page 1585](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1464](#)

CHAPTER 68

SNMP FAQs

- [Junos OS SNMP FAQ Overview on page 1591](#)
- [Junos OS SNMP FAQs on page 1592](#)

Junos OS SNMP FAQ Overview

This document presents the most frequently asked questions about the features and technologies used to implement SNMP services on Juniper Networks devices using the Junos operating system.

SNMP enables users to monitor network devices from a central location. Many network management systems (NMS) are based on SNMP, and support for this protocol is a key feature of most network devices.

Juniper Networks provides many different platforms that support SNMP on the Junos OS. The Junos OS includes an onboard SNMP agent that provides remote management applications with access to detailed information about the devices on the network.

A typical SNMP implementation contains three components:

- Managed devices – Such as routers and switches.
- SNMP agent – Process that resides on a managed device and communicates with the NMS.
- NMS – A combination of hardware and software used to monitor and administer the network; network device that runs SNMP manager software. Also referred to as an SNMP manager.

The SNMP agent exchanges network management information with the SNMP manager (NMS). The agent responds to requests for information and actions from the manager. The SNMP manager collects information about network connectivity, activity, and events by polling managed devices.

SNMP implementation in the Junos OS uses a master SNMP agent (known as an SNMP process or `snmpd`) that resides on the managed device. Various subagents reside on different modules of the Junos OS as well (such as the Routing Engine), and these subagents are managed by the `snmpd`.

Related Documentation

- [Junos OS SNMP FAQs on page 1592](#)

Junos OS SNMP FAQs

This Frequently Asked Questions technology overview covers these SNMP-related areas:

- [Junos OS SNMP Support FAQs on page 1592](#)
- [Junos OS MIBs FAQs on page 1593](#)
- [Junos OS SNMP Configuration FAQs on page 1600](#)
- [SNMPv3 FAQs on page 1604](#)
- [SNMP Interaction with Juniper Networks Devices FAQs on page 1606](#)
- [SNMP Traps and Informs FAQs on page 1608](#)
- [Junos OS Dual Routing Engine Configuration FAQs on page 1614](#)
- [SNMP Support for Routing Instances FAQs on page 1615](#)
- [SNMP Counters FAQs on page 1616](#)

Junos OS SNMP Support FAQs

This section presents frequently asked questions and answers related to SNMP support on Junos OS.

Which SNMP versions does Junos OS support?

Junos OS supports SNMP version 1 (SNMPv1), version 2 (SNMPv2c), and version 3 (SNMPv3). By default, SNMP is disabled on a Juniper Networks device.

Which ports (sockets) does SNMP use?

The default port for SNMP queries is port 161. The default port for SNMP traps and informs is port 162. The ports used by SNMP are configurable, and you can configure your system to use ports other than the defaults.

Is SNMP support different among the Junos OS platforms?

No, SNMP support is not different among the Junos OS platforms. SNMP configuration, interaction, and behavior are the same on any Junos OS device. The only difference that might occur across platforms is MIB support.

See also the *SNMP MIBs and Traps Reference* for a list of MIBs that are supported across the Junos OS platforms.

Does Junos OS support the user-based security model (USM)?

Yes, Junos OS supports USM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined USM. SNMPv3 USM provides message security through data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload.

Does Junos OS support the view-based access control model (VACM)?

Yes, Junos OS supports VACM as part of its support for SNMPv3. SNMPv3 contains more security measures than previous versions of SNMP, including providing a defined VACM. SNMPv3 VACM determines whether a specific type of access (read or write) to the management information is allowed.

Does Junos OS support SNMP informs?

Yes, Junos OS supports SNMP informs as part of its support for SNMPv3. SNMP informs are confirmed notifications sent from SNMP agents to SNMP managers when significant events occur on a network device. When an SNMP manager receives an inform, it sends a response to the sender to verify receipt of the inform.

Can I provision or configure a device using SNMP on Junos OS?

No, provisioning or configuring a device using SNMP is not allowed on Junos OS.

Related Documentation

Junos OS MIBs FAQs

This section presents frequently asked questions and answers related to Junos OS MIBs.

What is a MIB?

A management information base (MIB) is a table of definitions for managed objects in a network device. MIBs are used by SNMP to maintain standard definitions of all of the components and their operating conditions within a network device. Each object in the MIB has an identifying code called an object identifier (OID).

MIBs are either standard or enterprise-specific. Standard MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer.

For a list of supported standard MIBs, see “[Standard SNMP MIBs Supported by Junos OS](#)” on page 1409.

For a list of Juniper Networks enterprise-specific MIBs, see “[Enterprise-Specific SNMP MIBs Supported by Junos OS](#)” on page 1427.

Do MIB files reside on the Junos OS devices?

No, MIB files do not reside on the Junos OS devices. You must download the MIB files from the Juniper Networks Technical Publications page for the required Junos OS release: http://www.juniper.net/techpubs/en_US/release-independent/junos/mibs/mibs.html.

How do I compile and load the Junos OS MIBs onto an SNMP manager or NMS?

For your network management systems (NMSs) to identify and understand the MIB objects used by Junos OS, you must first load the MIB files to your NMS using a MIB compiler. A MIB compiler is a utility that parses the MIB information, such as the MIB object names, IDs, and data types for the NMS.

You can download the Junos OS MIB package from the Enterprise-Specific MIBs and Traps section at

http://www.juniper.net/techpubs/en_US/release-independent/junos/mibs/mibs.html or <http://www.juniper.net/techpubs/software/junos/index.html>.

The Junos OS MIB package has two folders: **StandardMibs**, containing standard MIBs supported on Juniper Networks devices, and **JuniperMibs**, containing Juniper Networks enterprise-specific MIBs. You *must* have the required standard MIBs downloaded and decompressed before downloading any enterprise-specific MIBs. There might be dependencies that require a particular standard MIB to be present on the compiler before loading a particular enterprise-specific MIB.

The Junos OS MIB package is available in **.zip** and **.tar** formats. Download the format appropriate for your requirements.

Use the following steps to load MIB files for devices running Junos OS:

1. Navigate to the appropriate Juniper Networks software download page and locate the **Enterprise MIBs** link under the **Enterprise-Specific MIBs and Traps** section.



NOTE: Although the link is titled **Enterprise MIBs**, both standard MIBs and enterprise-specific MIBs are available for download from this location.

2. Click the **TAR** or **ZIP** link to download the Junos OS MIB package.
3. Decompress the file (**.tar** or **.zip**) using an appropriate utility.



NOTE: Some commonly used MIB compilers are preloaded with standard MIBs. You can skip Step 4 and Step 5 and proceed to Step 6 if you already have the standard MIBs loaded on your system.

4. Load the standard MIB files from the **StandardMibs** folder.

Load the files in the following order:

- a. mib-SNMPv2-SMI.txt
 - b. mib-SNMPv2-TC.txt
 - c. mib-IANAifType-MIB.txt
 - d. mib-IANA-RTPROTO-MIB.txt
 - e. mib-rfc1907.txt
 - f. mib-rfc2011a.txt
 - g. mib-rfc2012a.txt
 - h. mib-rfc2013a.txt
 - i. mib-rfc2863a.txt
5. Load any remaining standard MIB files.



NOTE: You must follow the order specified in this procedure, and ensure that all standard MIBs are loaded before you load the enterprise-specific MIBs. There might be dependencies that require a particular standard MIB to be present on the compiler before loading a particular enterprise-specific MIB. Dependencies are listed in the **IMPORT** section of the MIB file.

6. After loading the standard MIBs, load the Juniper Networks enterprise-specific SMI MIB, **mib-jnx-smi.txt**, and the following optional SMI MIBs based on your requirements:
 - **mib-jnx-exp.txt**—(Recommended) for Juniper Networks experimental MIB objects
 - **mib-jnx-js-smi.txt**—(Optional) for Juniper Security MIB tree objects
 - **mib-jnx-ex-smi.txt**—(Optional) for EX Series Ethernet Switches
7. Load any remaining desired enterprise-specific MIBs from the **JuniperMibs** folder.



TIP: While loading a MIB file, if the compiler returns an error message indicating that any of the objects are undefined, open the MIB file using a text editor and ensure that all the MIB files listed in the **IMPORT** section are loaded on the compiler. If any of the MIB files listed in the **IMPORT** section are not loaded on the compiler, load the missing file or files first, then try to load the MIB file that failed.

The system might return an error if files are not loaded in a particular order.

What is SMI?

Structure of Management Information Version (SMI) is a subset of Abstract Syntax Notation One (ASN.1), which describes the structure of objects. SMI is the notation syntax, or “grammar”, that is the standard for writing MIBs.

Which versions of SMI does Junos OS support?

The Junos OS supports SMIV1 for SNMPv1 MIBs, and SMIV2 for SNMPv2c and enterprise MIBs.

Does Junos OS support MIB II?

Yes, Junos OS supports MIB II, the second version of the MIB standard.

The features of MIB II include:

- Additions that reflect new operational requirements.
- Backward compatibility with the original MIBs and SNMP.
- Improved support for multiprotocol entities.
- Improved readability.

Refer to the relevant release documentation for a list of MIBs that are supported. Go to <http://www.juniper.net/techpubs/software/junos/index.html>.

Are the same MIBs supported across all Juniper Networks devices?

There are some common MIBs supported by all the Junos OS devices, such as the Interface MIB (ifTable), System MIB, and Chassis MIB. Some MIBs are supported only by functionalities on specific platforms. For example, the Bridge MIB is supported on the EX Series Ethernet Switches and the SRX Series Services Gateways for the branch.

What is the system object identifier (SYSOID) of a device? How do I determine the SYSOID of my device?

The jnx-chas-defines (Chassis Definitions for Router Model) MIB has a **jnxProductName** branch for every Junos OS device. The system object ID of a device is identical to the object ID of the **jnxProductName** for the platform. For example, for an M7i Multiservice Edge Router, the jnxProductNameM7i is .1.3.6.1.4.1.2636.1.1.1.2.10 in the jnxProductName branch, which is identical to the SYSOID of the M7i (.1.3.6.1.4.1.2636.1.1.1.2.10).

How can I determine if a MIB is supported on a platform? How can I determine which MIBs are supported by a device?

MIBs device and platform support is listed on the Junos OS Technical Documentation index page. Go to <http://www.juniper.net/techpubs/software/junos/> and select your version or release of Junos OS. Navigate to the *SNMP MIBs and Traps Reference*. The *SNMP MIBs and Traps Reference* specifies which MIBs are supported on the different platforms.

What can I do if the MIB OID query is not responding?

There can be various reasons why the MIB OID query stops responding. One reason could be that the MIB itself is unresponsive. To verify that the MIB responds, use the **show snmp mib walk | get MIB name | MIB OID** command:

- If the MIB responds, the communication issue exists between the SNMP master and SNMP agent. Possible reasons for this issue include network issues, an incorrect community configuration, an incorrect SNMP configuration, and so on.
- If the MIB does not respond, enable SNMP **traceoptions** to log PDUs and errors. All incoming and outgoing SNMP PDUs are logged. Check the **traceoptions** output to see if there are any errors.

If you continue to have problems with the MIB OID query, technical product support is available through the Juniper Networks Technical Assistance Center (JTAC).

What is the enterprise branch number for Junos OS?

The enterprise branch number for Junos OS is 2636. Enterprise branch numbers are used in SNMP MIB configurations, and they are also known as SMI network management private enterprise codes.

Which MIB displays the hardware and chassis details on a Juniper Networks device?

The Chassis MIB (jnxchassis.mib) displays the hardware and chassis details for each Juniper Networks device. It provides information about the router and its components. The Chassis MIB objects represent each component and its status.

For more information about enterprise-specific Chassis MIBs, see *Chassis MIBs* in the *Junos OS SNMP MIBs and Traps Reference* document.

Which MIB objects can I query to determine the CPU and memory utilization of the Routing Engine, Flexible PIC Concentrator (FPC), and PIC components on a device?

Query the Chassis MIB objects `jnxOperatingMemory`, `jnxOperatingtBuffer`, and `jnxOperatingCPU` to find out the CPU and memory utilization of the hardware components of a device.

Is the interface index (ifIndex) persistent?

The ifIndex is persistent when reboots occur if the Junos OS version remains the same, meaning the values assigned to the interfaces in the ifIndex do not change.

When there is a software upgrade, the device tries to keep the ifIndex persistent on a best effort basis. For Junos OS Release 10.0 and earlier, the ifIndex is not persistent when there is a software upgrade to Junos OS Release 10.1 and later.

Is it possible to set the ifAdminStatus?

SNMP is not allowed to set the ifAdminStatus.

Which MIB objects support SNMP set operations?

The Junos OS SNMP set operations are supported in the following MIB tables and variables:

- snmpCommunityTable
- eventTable
- alarmTable
- snmpTargetAddrExtTable
- jnxPingCtlTable
- pingCtlTable
- traceRouteCtlTable
- jnxTraceRouteCtlTable
- sysContact.O
- sysName.O
- sysLocation.O
- pingMaxConcurrentRequests.O
- traceRouteMaxConcurrentRequests.O
- usmUserSpinLock

- usmUserOwnAuthKeyChange
- usmUserPublic
- vacmSecurityToGroupTable (vacmGroupName, vacmSecurityToGroupStorageType, and vacmSecurityToGroupStatus)
- vacmAccessTable (vacmAccessContextMatch, vacmAccessReadViewName, vacmAccessWriteViewName, vacmAccessNotifyViewName, vacmAccessStorageType, and vacmAccessStatus)
- vacmViewSpinLock
- vacmViewTreeFamilyTable (vacmViewTreeFamilyMask, vacmViewTreeFamilyType, vacmViewTreeFamilyStorageType, and vacmViewTreeFamilyStatus)

Does Junos OS support remote monitoring (RMON)?

Yes, Junos OS supports RMON as defined in RFC 2819, *Remote Network Monitoring Management Information Base*. However, remote monitoring version 2 (RMON 2) is not supported.

Can I use SNMP to determine the health of the processes running on the Routing Engine?

Yes, you can use SNMP to determine the health of the Routing Engine processes by configuring the health monitoring feature. On Juniper Networks devices, RMON alarms and events provide much of the infrastructure needed to reduce the polling overhead from the NMS. However, you must set up the NMS to configure specific MIB objects into RMON alarms. This often requires device-specific expertise and customizing the monitoring application. Additionally, some MIB object instances that need monitoring are set only at initialization, or they change at runtime and cannot be configured in advance.

To address these issues, the health monitor extends the RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances, such as file system usage, CPU usage, and memory usage, and includes support for unknown or dynamic object instances, such as Junos OS software processes.

To display the health monitoring configuration, use the **show snmp health-monitor** command:

```
user@host> show snmp health-monitor
interval 300;
rising-threshold 90;
falling-threshold 80;
```

When you configure the health monitor, monitoring information for certain object instances is available, as shown in [Table 124](#).

Table 124: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed.1	Monitors the following file system on the router or switch: /dev/ad0s1a: This is the root file system mounted on /.
jnxHrStoragePercentUsed.2	Monitors the following file system on the router or switch: /dev/ad0s1e: This is the configuration file system mounted on /config.
jnxOperatingCPU (RE0)	Monitor CPU usage for Routing Engines RE0 and RE1. The index values assigned to the Routing Engines depend on whether the Chassis MIB uses a zero-based or a ones-based indexing scheme. Because the indexing scheme is configurable, the correct index is determined whenever the router is initialized and when there is a configuration change. If the router or switch has only one Routing Engine, the alarm entry monitoring RE1 is removed after five failed attempts to obtain the CPU value.
jnxOperatingCPU (RE1)	
jnxOperatingBuffer (RE0)	Monitor the amount of memory available on Routing Engines RE0 and RE1. Because the indexing of this object is identical to that used for jnxOperatingCPU, index values are adjusted depending on the indexing scheme used in the Chassis MIB. As with jnxOperatingCPU, the alarm entry monitoring RE1 is removed if the router or switch has only one Routing Engine.
jnxOperatingBuffer (RE1)	
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS software process. Multiple instances of the same process are monitored and indexed separately.
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS software process. Multiple instances of the same process are monitored and indexed separately.

The system log entries generated for any health monitor events, such as thresholds crossed and errors, have a corresponding **HEALTHMONITOR** tag rather than a generic **SNMPD_RMON_EVENTLOG** tag. However, the health monitor sends generic **RMON risingThreshold** and **fallingThreshold** traps.

Are the Ping MIBs returned in decimal notation and ASCII?

Yes, both decimal notation and ASCII are supported, which is the standard implementation in SNMP. All strings are ASCII encoded.

The following example displays the Ping MIB in hexadecimal notation:

```
pingCtlTargetAddress.2.69.72.9.116.99.112.115.97.109.112.108.101 = 0a fa 01 02
```

This translates to ASCII:

```
pingCtlTargetAddress."EH"."tcpsample" = 0a fa 01 02
2=length of the string
69=E
72=H
9=length of second string
116=t
99 =c
112=p
115=s
```

```
97=a
109=m
112 =p
108 =l
101 =e
```

As of Junos OS Release 9.6 and later, the Junos OS CLI returns ASCII values using the command **show snmp mib get | get-next | walk ascii**.

The following example shows the output with the ASCII option:

```
user@host> show snmp mib walk pingCtlTargetAddress ascii
pingCtlTargetAddress."EH"."httpgetsample" = http://www.yahoo.com
pingCtlTargetAddress."p1"."t2" = 74 c5 b3 06
pingCtlTargetAddress."p1"."t3" = 74 c5 b2 0c
```

The following example shows the output without the ASCII option:

```
user@host> show snmp mib walk pingCtlTargetAddress
pingCtlTargetAddress.2.69.72.13.104.116.116.112.103.101.116.115.97.109.112.108.101
= http://www.yahoo.com
pingCtlTargetAddress.2.112.49.2.116.50 = 74 c5 b3 06
pingCtlTargetAddress.2.112.49.2.116.51 = 74 c5 b2 0c
```

You can convert decimal and ASCII values using a decimal ASCII chart like the one at <http://www.asciichart.com>.

Is IPv6 supported by the Ping MIB for remote operations?

No, IPv6 is not supported.

Is there an SNMP MIB to show Address Resolution Protocol (ARP) table information? Are both IP and MAC addresses displayed in the same table?

Yes, the Junos OS supports the standard MIB **ipNetToMediaTable**, which is described in RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*. This table is used for mapping IP addresses to their corresponding MAC addresses.

Related Documentation

Junos OS SNMP Configuration FAQs

This section presents frequently asked questions and answers related to Junos OS SNMP configuration.

Can the Junos OS be configured for SNMPv1 and SNMPv3 simultaneously?

Yes, SNMP has backward compatibility, meaning that all three versions can be enabled simultaneously.

Can I filter specific SNMP queries on a device?

Yes, you can filter specific SNMP queries on a device using **exclude** and **include** statements.

The following example shows a configuration that blocks read-write operation on all OIDs under .1.3.6.1.2.1.1 for the community **test**:

```
user@host# show snmp
view system-exclude {
  oid .1.3.6.1.2.1.1 exclude;
  oid .1 include;
}
community test {
  view system-exclude;
  authorization read-write;
}
```

Can I change the SNMP agent engine ID?

Yes, the SNMP agent engine ID can be changed to the MAC address of the device, the IP address of the device, or any other desired value. Several examples are included here.

The following example shows how to use the MAC address of a device as the SNMP agent engine ID:

```
user@host# show snmp
engine-id {
  use-mac-address;
}
```

The following example shows how to use the IP address of a device as the SNMP agent engine ID:

```
user@host# show snmp
engine-id {
  use-default-ip-address;
}
```

The following example shows the use of a selected value, **AA** in this case, as the SNMP agent engine ID of a device:

```
user@host# show snmp
engine-id {
  local AA;
}
```

How can I configure a device with dual Routing Engines or a chassis cluster (SRX Series Services Gateways) for continued communication during a switchover?

When configuring for continued communication, the SNMP configuration should be identical between the Routing Engines. However, it is best to have separate Routing Engine IDs configured for each Routing Engine, especially when using SNMPv3.

The following example shows the configuration of the Routing Engines in a dual Routing Engine device. Notice that the Routing Engine IDs are set to the MAC addresses for each Routing Engine:

```
user@host# show groups
re0 {
  system {
    host-name PE3-re0;
  }
}
```

```
interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address 116.197.178.14/27;
        address 116.197.178.29/27 {
          master-only;
        }
      }
    }
  }
}
snmp {
  engine-id {
    use-mac-address;
  }
}
}
rel {
  system {
    host-name PE3-rel;
  }
  interfaces {
    fxp0 {
      unit 0 {
        family inet {
          address 116.197.178.11/27;
          address 116.197.178.29/27 {
            master-only;
          }
        }
      }
    }
  }
  snmp {
    engine-id {
      use-mac-address;
    }
  }
}
```

The following is an example of an SNMPv3 configuration on a dual Routing Engine device:

```
user@host> show snmp name host1
v3 {
  vacm {
    security-to-group {
      security-model usm {
        security-name test123 {
          group test1;
        }
        security-name juniper {
          group test1;
        }
      }
    }
  }
}
```

```

access {
  group test1 {
    default-context-prefix {
      security-model any {
        security-level authentication {
          read-view all;
        }
      }
    }
    context-prefix MGMT_10 {
      security-model any {
        security-level authentication {
          read-view all;
        }
      }
    }
  }
}

target-address server1 {
  address 116.197.178.20;
  tag-list router1;
  routing-instance MGMT_10;
  target-parameters test;
}

target-parameters test {
  parameters {
    message-processing-model v3;
    security-model usm;
    security-level authentication;
    security-name juniper;
  }
  notify-filter filter1;
}

notify server {
  type trap;
  tag router1;
}

notify-filter filter1 {
  oid .1 include;
}

view all {
  oid .1 include;
}

community public {
  view all;
}

community comm1;
community comm2;
community comm3 {
  view all;
  authorization read-only;
  logical-system LDP-VPLS {
    routing-instance vpls-server1;
  }
}

```

```
trap-group server1 {
  targets {
    116.197.179.22;
  }
}
routing-instance-access;
traceoptions {
  flag all;
}
```

How can I track SNMP activities?

SNMP trace operations track activity of SNMP agents and record the information in log files.

A sample **traceoptions** configuration might look like this:

```
[edit snmp]
user@host# set traceoptions flag all
```

When the **traceoptions flag all** statement is included at the **[edit snmp]** hierarchy level, the following log files are created:

- snmpd
- mib2d
- rmopd

Related Documentation

- [Junos OS SNMP Support FAQs on page 1592](#)
- [Junos OS MIBs FAQs on page 1593](#)
- [SNMPv3 FAQs on page 1604](#)
- [SNMP Interaction with Juniper Networks Devices FAQs on page 1606](#)
- [SNMP Traps and Informs FAQs on page 1608](#)
- [SNMP Support for Routing Instances FAQs on page 1615](#)
- [SNMP Counters FAQs on page 1616](#)

SNMPv3 FAQs

This section presents frequently asked questions and answers related to SNMPv3.

Why is SNMPv3 important?

SNMP v3 provides enhanced security compared to the other versions of SNMP. It provides authentication and encryption of data. Enhanced security is important for managing devices at remote sites from the management stations.

In my system, the MIB object snmpEngineBoots is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Yes, this is the expected behavior. Each Routing Engine runs its own SNMP process (snmpd), allowing each Routing Engine to maintain its own engine boots. However, if both routing engines have the same engine ID and the routing engine with lesser **snmpEngineBoots** value is selected as the master routing engine during the switchover process, the **snmpEngineBoots** value of the master routing engine is synchronized with the **snmpEngineBoots** value of the other routing engine.

Do I need the SNMP manager engine object identifier (OID) for informs?

Yes, the engine OID of the SNMP manager is required for authentication, and informs do not work without it.

I see the configuration of informs under the [edit snmp v3] hierarchy. Does this mean I cannot use informs with SNMPv2c?

Informs can be used with SNMPv2c. The following example shows the basic configuration for SNMPv3 informs on a device (note that the authentication and privacy is set to none):

```
[edit snmp]
v3 {
  usm {
    remote-engine 00000063000100a2c0a845b3 {
      user RU2_v3_sha_none {
        authentication-none;
        privacy-none;
      }
    }
  }
  vacm {
    security-to-group {
      security-model usm {
        security-name RU2_v3_sha_none {
          group g1_usm_auth;
        }
      }
    }
  }
  access {
    group g1_usm_auth {
      default-context-prefix {
        security-model usm {
          security-level authentication {
            read-view all;
            write-view all;
            notify-view all;
          }
        }
      }
    }
  }
}
target-address TA2_v3_sha_none {
  address 192.168.69.179;
  tag-list tl1;
  address-mask 255.255.252.0;
  target-parameters TP2_v3_sha_none;
```

```
}
target-parameters TP2_v3_sha_none {
  parameters {
    message-processing-model v3;
    security-model usm;
    security-level none;
    security-name RU2_v3_sha_none;
  }
  notify-filter nfl;
}
notify N1_all_tl1_informs {
  type inform; # Replace "inform" with "trap" to convert informs to traps.
  tag tl1;
}
notify-filter nfl {
  oid .1 include;
}
view all {
  oid .1 include;
}
}
```

You can convert the SNMPv3 informs to traps by setting the value of the **type** statement at the **[edit snmp v3 notify N1_all_tl1_informs]** hierarchy level to **trap** as shown in the following example:

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

Related Documentation

SNMP Interaction with Juniper Networks Devices FAQs

This section presents frequently asked questions and answers related to how SNMP interacts with Juniper Networks devices.

How frequently should a device be polled? What is a good polling rate?

It is difficult to give an absolute number for the rate of SNMP polls per second since the rate depends on the following two factors:

- The number of variable bindings in a protocol data unit (PDU)
- The response time for an interface from the Packet Forwarding Engine

In a normal scenario where no delay is being introduced by the Packet Forwarding Engine and there is one variable per PDU (a Get request), the response time is 130+ responses per second. However, with multiple variables in an SNMP request PDU (30 to 40 for GetBulk requests), the number of responses per second is much less. Because the Packet Forwarding Engine load can vary for each system, there is greater variation in how frequently a device should be polled.

Frequent polling of a large number of counters, especially statistics, can impact the device. We recommend the following optimization on the SNMP managers:

- Use the row-by-row polling method, not the column-by-column method.
- Reduce the number of variable bindings per PDU.
- Increase timeout values in polling and discovery intervals.
- Reduce the incoming packet rate at the SNMP process (snmpd).

For better SNMP response on the device, the Junos OS does the following:

- Filters out duplicate SNMP requests.
- Excludes interfaces that are slow in response from SNMP queries.

One way to determine a rate limit is to note an increase in the **Currently Active** count from the **show snmp statistics extensive** command.

The following is a sample output of the **show snmp statistics extensive** command:

```
user@host> show snmp statistics extensive
SNMP statistics:
  Input:
    Packets: 226656, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 1967606, Total set varbinds: 0,
    Get requests: 18478, Get nexts: 75794, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 27084, Duplicate request drops: 0
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 0
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
  Output:
    Packets: 226537, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 226155, Traps: 382
  SA Control Blocks:
    Total: 222984, Currently Active: 501, Max Active: 501,
    Not found: 0, Timed Out: 0, Max Latency: 25
  SA Registration:
    Registers: 0, Deregisters: 0, Removes: 0
  Trap Queue Stats:
    Current queued: 0, Total queued: 0, Discards: 0, Overflows: 0
  Trap Throttle Stats:
    Current throttled: 0, Throttles needed: 0
  Snmp Set Stats:
    Commit pending failures: 0, Config lock failures: 0
    Rpc failures: 0, Journal write failures: 0
    Mgd connect failures: 0, General commit failures: 0
```

Does SNMP open dynamic UDP ports? Why?

The SNMP process opens two additional ports (sockets): one for IPv4 and one for IPv6. This enables the SNMP process to send traps.

I am unable to perform a MIB walk on the ifIndex. Why is this?

Any variable bindings or values with an access level of **not-accessible** cannot be queried directly because they are part of other variable bindings in the SNMP MIB table. The ifIndex has an access level of **not-accessible**. Therefore, it cannot be accessed directly because it is part of the variable bindings. However, the ifIndex can be accessed indirectly through the variable bindings.

I see SNMP_IPC_READ_ERROR messages when the SNMP process restarts on my system and also during Routing Engine switchover. Is this acceptable?

Yes, it is acceptable to see **SNMP_IPC_READ_ERROR** messages when the SNMP process is restarted, the system reboots, or during a Routing Engine switchover. If all the processes come up successfully and the SNMP operations are working properly, then these messages can be ignored.

What is the source IP address used in the response PDUs for SNMP requests? Can this be configured?

The source IP address used in the response PDUs for SNMP requests is the IP address of the outgoing interface to reach the destination. The source IP address cannot be configured for responses. It can only be configured for traps.

**Related
Documentation**

SNMP Traps and Informs FAQs

This section presents frequently asked questions and answers related to SNMP traps and informs.

Does the Junos OS impose any rate limiting on SNMP trap generation?

The Junos OS implements a trap-queuing mechanism to limit the number of traps that are generated and sent.

If a trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts occur at progressive intervals of 1, 2, 4, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is 10. After 10 unsuccessful attempts, the destination queue and all traps in the queue are deleted.

Junos OS also has a throttle threshold mechanism to control the number of traps sent (default 500 traps) during a particular throttle interval (default 5 seconds). This helps ensure consistency in trap traffic, especially when a large number of traps are generated due to interface status changes.

The throttle interval begins when the first trap arrives at the throttle. All traps within the throttle threshold value are processed, and traps exceeding the threshold value are queued. The maximum size of all trap queues (the throttle queue and the destination

queue) is 40,000 traps. The maximum size of any one queue is 20,000 traps. When a trap is added to the throttle queue, or if the throttle queue has exceeded the maximum size, the trap is moved to the top of the destination queue. Further attempts to send the trap from the destination queue are stopped for a 30-second period, after which the destination queue restarts sending the traps.



NOTE: For the Juniper Networks EX Series Ethernet Switch, the maximum size of all trap queues (the throttle queue and the destination queue) is 1,000 traps. The maximum size for any one queue on the EX Series is 500 traps.

I did not see a trap when I had a syslog entry with a critical severity. Is this normal? Can it be changed?

Not every syslog entry with critical severity is a trap. However, you can convert any syslog entry to a trap using the **event-options** statement.

The following example shows how to configure a **jnxSyslogTrap** whenever an **rpd_ldp_nbrdown** syslog entry message error occurs.

```
user@host> show event-options
policy snmptrap {
  events rpd_ldp_nbrdown;
  then {
    raise-trap;
  }
}
```

Are SNMP traps compliant with the Alarm Reporting Function (X.733) on the Junos OS?

No, SNMP traps on the Junos OS are not X.733 compliant.

Can I set up filters for traps or informs?

Traps and informs can be filtered based on the trap category and the object identifier. You can specify categories of traps to receive per host by using the **categories** statement at the **[edit snmp trap-group trap-group]** hierarchy level. Use this option when you want to monitor only specific modules of the Junos OS.

The following example shows a sample configuration for receiving only **link**, **vrrp-events**, **services**, and **otn-alarms** traps:

```
[edit snmp]
trap-group jnpr {
  categories {
    link;
    vrrp-events;
    services;
    otn-alarms;
  }
  targets {
    192.168.69.179;
  }
}
```

```
}
```

The Junos OS also has a more advanced filter option (**notify-filter**) for filtering specific traps or a group of traps based on their object identifiers.

The SNMPv3 configuration also supports filtering of SNMPv1 and SNMPv2 traps and excluding Juniper Networks enterprise-specific configuration management traps, as shown in the following configuration example:

```
[edit snmp]
v3 {
  vacm {
    security-to-group {
      security-model v2c {
        security-name sn_v2c_trap {
          group gr_v2c_trap;
        }
      }
    }
  }
  access {
    group gr_v2c_trap {
      default-context-prefix {
        security-model v2c {
          security-level none {
            read-view all;
            notify-view all;
          }
        }
      }
    }
  }
}

target-address TA_v2c_trap {
  address 10.209.196.166;
  port 9001;
  tag-list tg1;
  target-parameters TP_v2c_trap;
}

target-parameters TP_v2c_trap {
  parameters {
    message-processing-model v2c;
    security-model v2c;
    security-level none;
    security-name sn_v2c_trap;
  }
  notify-filter nf1;
}

notify v2c_notify {
  type trap;
  tag tg1;
}

notify-filter nf1 {
  oid .1.3.6.1.4.1.2636.4.5 exclude;
  oid .1 include;
}

snmp-community index1 {
```

```

community-name "$9$tDLi01h7Nbw2axN"; ## SECRET-DATA
security-name sn_v2c_trap;
tag tgl;
}
view all {
oid .1 include;
}
}

```

Can I simulate traps on a device?

Yes, you can use the **request snmp spoof-trap *trap name*** command for simulating a trap to the NMS that normally receives your device's traps. You can also add required values using the **variable-bindings** parameter.

The following example shows how to simulate a trap to the local NMS using variable bindings:

```

user@host> request snmp spoof-trap linkDown variable-bindings "ifIndex[116]=116,
ifAdminStatus[116]=1 ,ifOperStatus[116]=2 ,ifName[116]=ge-1/0/1"

```

How do I generate a warm start SNMPv1 trap?

When the SNMP process is restarted under normal conditions, a warm start trap is generated if the system up time is more than 5 minutes. If the system up time is less than 5 minutes, a cold start trap is generated.

The NMS sees only the MIB OIDs and numbers, but not the names of the SNMP traps. Why?

Before the NMS can recognize the SNMP trap details, such as the names of the traps, it must first compile and understand the MIBs and then parse the MIB OIDs.

In the Junos OS, how can I determine to which category a trap belongs?

For a list of common traps and their categories, see *Juniper Networks Enterprise-Specific SNMP Version 1 Traps* and *Juniper Networks Enterprise-Specific SNMP Version 2 Traps* in the *Junos OS SNMP MIBs and Traps Reference* document.

Can I configure a trap to include the source IP address?

Yes, you can configure the **source-address**, **routing-instance**, or **logical-instance** name for the source IP address using the **trap-options** command:

```

user@host> show snmp trap-options
source-address 10.1.1.1;

```

Can I create a custom trap?

Yes, you can use the **jnxEventTrap** event script to create customized traps as needed.

In the following example, a Junos OS operations (op) script is triggered when a **UI_COMMIT_NOT_CONFIRMED** event is received. The Junos OS op script matches the complete message of the event and generates an SNMP trap.

Example: Junos OS Op Script

```

version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";

param $event;
param $message;

match / {

    /*
     * trapm utility wants the following characters in the value to be escaped
     * '[', ']', ' ', '=', and ','
     */
    var $event-escaped = {
        call escape-string($text = $event, $vec = '[] =,');
    }

    var $message-escaped = {
        call escape-string($text = $message, $vec = '[] =,');
    }

    <op-script-results> {
    var $rpc = <request-snmp-spoof-trap> {
        <trap> "jnxEventTrap";
        <variable-bindings> "jnxEventTrapDescr[0]='Event-Trap' , "
        _ "jnxEventAvAttribute[1]='event' , "
        _ "jnxEventAvValue[1]='" _ $event-escaped _ "' , "
        _ "jnxEventAvAttribute[2]='message' , "
        _ "jnxEventAvValue[1]='" _ $message-escaped _ "'";
    }

    var $res = jcs:invoke($rpc);
    }

template escape-string ($text, $vec) {

    if (jcs:empty($vec)) {
        expr $text;

    } else {
        var $index = 1;
        var $from = substring($vec, $index, 1);
        var $changed-value = {
            call replace-string($text, $from) {
                with $to = {
                    expr "\\\";
                    expr $from;
                }
            }
        }

        call escape-string($text = $changed-value, $vec = substring($vec, $index
+ 1));
    }
}

```

```

template replace-string ($text, $from, $to) {

    if (contains($text, $from)) {
        var $before = substring-before($text, $from);
        var $after = substring-after($text, $from);
        var $prefix = $before _ $to;

        expr $before;
        expr $to;
        call replace-string($text = $after, $from, $to);

    } else {
        expr $text;
    }
}

```

After creating your customized trap, you must configure a policy on your device to tell the device what actions to take after it receives the trap.

Here is an example of a configured policy under the **[edit event-options]** hierarchy:

```

[edit event-options]
user@host> show
policy trap-on-event {
    events UI_COMMIT_NOT_CONFIRMED;
    attributes-match {
        UI_COMMIT_NOT_CONFIRMED.message matches complete;
    }
    then {
        event-script ev-syslog-trap.junos-op {
            arguments {
                event UI_COMMIT_NOT_CONFIRMED;
                message "${$.message}";
            }
        }
    }
}

```

Can I disable link up and link down traps on interfaces?

Yes, link up and link down traps can be disabled in the interface configuration. To disable the traps, use the **no-traps** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** and **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]** hierarchies for physical and logical interfaces.

```
(traps | no-traps);
```

I see the link up traps on logical interfaces, but I do not see the link down traps. Is this normal behavior?

For Ethernet and ATM types of interfaces, Junos OS does not send link down traps for a logical interface if the physical interface is down to prevent flooding alarms for the same root cause. However, when the physical interface and logical interfaces come back up, traps are sent indicating link up. This is because the physical interface coming up does not necessarily mean the logical interfaces are also coming up.

For SONET types of interfaces with PPP encapsulation, Junos OS does send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For SONET types of interfaces with HDLC encapsulation, Junos OS does not send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For channelize interfaces with PPP encapsulation, Junos OS does send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

For channelize interfaces with HDLC encapsulation, Junos OS does not send link down traps for a logical interface if the physical interface is down. When the physical interface and logical interfaces come back up, traps are sent for both the physical and logical interfaces indicating link up.

Related Documentation

Junos OS Dual Routing Engine Configuration FAQs

This section presents frequently asked questions and answers related to the configuration of dual Routing Engines.

The SNMP configuration should be identical between the Routing Engines when configuring for continued communication. However, we recommend having separate Routing Engine IDs configured for each Routing Engine, when using SNMPv3.

In my system, the MIB object `snmpEngineBoots` is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Yes. This is the normal behavior. Each Routing Engine runs its own SNMP process (`snmpd`) agent, allowing each Routing Engine to maintain its own engine boots.

Is there a way to identify that an address belongs to RE0, RE1, or the master Routing Engine management interface (`fxp0`) by looking at an SNMP walk?

No. When you do an SNMP walk on the device, it only displays the master Routing Engine management interface address.

What is the best way to tell if the current IP address belongs to `fxp0` or a Routing Engine, from a CLI session?

Routing Engines are mapped with the `fxp0` interface. This means that when you query RE0, the `ifTable` reports the `fxp0` interface address of RE0 only. Similarly, if you query RE1, the `ifTable` reports the `fxp0` interface address of RE1 only.

When there is a failover, the master hostname is changed since the hostname belongs to the Routing Engine. Is this correct?

Yes. You can configure the same hostname or different hostnames. Either would work.

If only the master IP address is configured (for example, 192.168.2.5), and the **sysDescr.0** object has the same string configured on both of the Routing Engines, then even after a switchover, the **sysDescr.0** object returns the same value. The following sample shows the results you get by using the **snmpget** command:

```
bng-junos-pool02: /c/svivek/PR_BRANCH/src> snmpget -c jnpr -v2c 192.168.2.5
sysDescr.0 system.sysDescr.0 = foo
```

SNMP Support for Routing Instances FAQs

This section presents frequently asked questions and answers related to how SNMP supports routing instances.

Can the SNMP manager access data for routing instances?

Yes, the Junos OS enables SNMP managers for all routing instances to request and manage SNMP data related to the corresponding routing instances and logical system networks.

Two different routing instance behaviors can occur, depending on where the clients originate:

- Clients from routing instances other than the default can access MIB objects and perform SNMP operations only on the logical system networks to which they belong.
- Clients from the default routing instance can access information related to all routing instances and logical system networks.

Routing instances are identified by either the context field in SNMPv3 requests or encoded in the community string in SNMPv1 or SNMPv2c requests.

When encoded in a community string, the routing instance name appears first and is separated from the actual community string by the @ character.

To avoid conflicts with valid community strings that contain the @ character, the community is parsed only if typical community string processing fails. For example, if a routing instance named **RI** is configured, an SNMP request with **RI@public** is processed within the context of the **RI** routing instance. Access control (including views, source address restrictions, and access privileges) is applied according to the actual community string (the set of data after the @ character—in this case **public**). However, if the community string **RI@public** is configured, the PDU is processed according to that community, and the embedded routing instance name is ignored.

Logical systems perform a subset of the actions of a physical router and have their own unique routing tables, interfaces, policies, and routing instances. When a routing instance is defined within a logical system, the logical system name must be encoded along with the routing instance using a slash (/) to separate the two. For example, if the routing instance **RI** is configured within the logical system **LS**, that routing instance must be encoded within a community string as **LS/RI@public**. When a routing instance is configured outside a logical system (within the default logical system), no logical system name, or / character, is needed.

Additionally, when a logical system is created, a default routing instance named **default** is always created within the logical system. This name should be used when querying data for that routing instance, for example **LS/default@public**. For SNMPv3 requests, the name **logical system/routing instance** should be identified directly in the context field.

Can I access a list of all routing instances on a device?

Yes, you can access a list of all the routing instances on a device using the `vacmContextName` object in the SNMP-VIEW-BASED-ACM MIB. In SNMP, each routing instance becomes a VACM context; this is why the routing instances appear in the `vacmContextName` object.

Can I access a default routing instance from a client in another logical router or routing instance?

No, the SNMP agent can only access data of the logical router to which it is connected.

Related Documentation

SNMP Counters FAQs

This section presents frequently asked questions and answers related to SNMP counters.

Which MIB should I use for interface counters?

Interface management over SNMP is based on two tables: the **ifTable** and its extension the **ifXTable**. Both are described in RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* and RFC 2233, *The Interfaces Group MIB using SMIv2*.

Interfaces can have several layers, depending on the media, and each sublayer is represented by a separate row in the table. The relationship between the higher layer and lower layers is described in the **ifStackTable**.

The **ifTable** defines 32-bit counters for inbound and outbound octets (`ifInOctets/ifOutOctets`), packets (`ifInUcastPkts/ifOutUcastPkts`, `ifInNUcastPkts/ifOutNUcastPkts`), errors, and discards.

The **ifXTable** provides similar 64-bit counters, also called high capacity (HC) counters, for inbound and outbound octets (`ifHCInOctets/ifHCOctets`) and inbound packets (`ifHCInUcastPkts`).

When should 64-bit counters be used?

It is always good to use 64-bit counters because they contain statistics for both low and high capacity components.

Are the SNMP counters `ifInOctets` and `ifOutOctets` the same as the command `reference show interfaces statistics in and out counters`?

Yes, these are the same, but only if SNMP is enabled when the router boots up. If you power on a Juniper Networks device and then enable SNMP, the SNMP counters start

from 0. SNMP counters do not automatically receive their statistics from the **show** command output. Similarly, using the **clear statistics** command does not clear the statistics that the SNMP counters collected, which can cause a discrepancy in the data that is seen by both processes.

Do the SNMP counters ifInOctets and ifOutOctets include the framing overhead for Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC)?

Yes.

**Related
Documentation**

PART 18

Remote Monitoring (RMON) with SNMP

- [RMON Overview on page 1621](#)
- [Configuring RMON Alarms and Events on page 1625](#)
- [Monitoring RMON Alarms and Events on page 1633](#)
- [Using RMON to Monitor Network Service Quality on page 1639](#)

CHAPTER 69

RMON Overview

- [Understanding RMON Alarms on page 1621](#)
- [Understanding RMON Events on page 1623](#)

Understanding RMON Alarms

An RMON alarm identifies:

- A specific MIB object that is monitored.
- The frequency of sampling.
- The method of sampling.
- The thresholds against which the monitored values are compared.

An RMON alarm can also identify a specific **eventTable** entry to be triggered when a threshold is crossed.

Configuration and operational values are defined in **alarmTable** in RFC 2819. Additional operational values are defined in Juniper Networks enterprise-specific extensions to **alarmTable** (**jnxRmonAlarmTable**).

This topic covers the following sections:

- [alarmTable on page 1621](#)
- [jnxRmonAlarmTable on page 1622](#)

alarmTable

alarmTable in the RMON MIB allows you to monitor and poll the following:

- **alarmIndex**—The index value for **alarmTable** that identifies a specific entry.
- **alarmInterval**—The interval, in seconds, over which data is sampled and compared with the rising and falling thresholds.
- **alarmVariable**—The MIB variable that is monitored by the alarm entry.
- **alarmSampleType**—The method of sampling the selected variable and calculating the value to be compared against the thresholds.

- **alarmValue**—The value of the variable during the last sampling period. This value is compared with the rising and falling thresholds.
- **alarmStartupAlarm**—The alarm sent when the entry is first activated.
- **alarmRisingThreshold**—The upper threshold for the sampled variable.
- **alarmFallingThreshold**—The lower threshold for the sampled variable.
- **alarmRisingEventIndex**—The **eventTable** entry used when a rising threshold is crossed.
- **alarmFallingEventIndex**—The **eventTable** entry used when a falling threshold is crossed.
- **alarmStatus**—Method for adding and removing entries from the table. It can also be used to change the state of an entry to allow modifications.



NOTE: If this object is not set to **valid**, the associated event alarm does not take any action.

jnxRmonAlarmTable

The **jnxRmonAlarmTable** is a Juniper Networks enterprise-specific extension to **alarmTable**. It provides additional operational information and includes the following objects:

- **jnxRmonAlarmGetFailCnt**—The number of times the internal **Get** request for the variable monitored by this entry has failed.
- **jnxRmonAlarmGetFailTime**—The value of **sysUpTime** when an internal **Get** request for the variable monitored by this entry last failed.
- **jnxRmonAlarmGetFailReason**—The reason an internal **Get** request for the variable monitored by this entry last failed.
- **jnxRmonAlarmGetOkTime**—The value of **sysUpTime** when an internal **Get** request for the variable monitored by this entry succeeded and the entry left the **getFailure** state.
- **jnxRmonAlarmState**—The current state of this RMON alarm entry.

To view the Juniper Networks enterprise-specific extensions to the RMON Events and Alarms and Event MIB, see

http://www.juniper.net/techpubs/en_US/junos10.3/topics/reference/mibs/mib-jnx-rmon.txt.

For more information about the Juniper Networks enterprise-specific extensions to the RMON Events and Alarms MIB, see “*RMON Events and Alarms MIB*” in the *Network Management Administration Guide for Routing Devices*.

Related Documentation

- [Understanding RMON Events on page 1623](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [Using alarmTable to Monitor MIB Objects on page 1633](#)

Understanding RMON Events

An RMON event allows you to log the crossing of thresholds of other MIB objects. It is defined in **eventTable** for the RMON MIB.

This section covers the following topics:

- [eventTable on page 1623](#)

eventTable

eventTable contains the following objects:

- **eventIndex**—An index that uniquely identifies an entry in **eventTable**. Each entry defines one event that is generated when the appropriate conditions occur.
- **eventDescription**—A comment describing the event entry.
- **eventType**—Type of notification that the probe makes about this event.
- **eventCommunity**—Trap group used if an SNMP trap is to be sent. If **eventCommunity** is not configured, a trap is sent to each trap group configured with the **rmon-alarm** category.
- **eventLastTimeSent**—Value of **sysUpTime** when this event entry last generated an event.
- **eventOwner**—Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.
- **eventStatus**—Status of this event entry.



NOTE: If this object is not set to valid, no action is taken by the associated event entry. When this object is set to valid, all previous log entries associated with this entry (if any) are deleted.

Related Documentation

- [Understanding RMON Alarms on page 1621](#)
- [Configuring an Event Entry and Its Attributes on page 1630](#)

Configuring RMON Alarms and Events

- [Understanding RMON Alarms and Events Configuration on page 1625](#)
- [Minimum RMON Alarm and Event Entry Configuration on page 1626](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [Configuring an Event Entry and Its Attributes on page 1630](#)
- [Example: Configuring an RMON Alarm and Event Entry on page 1631](#)

Understanding RMON Alarms and Events Configuration

Junos OS supports monitoring routers from remote devices. These values are measured against thresholds and trigger events when the thresholds are crossed. You configure remote monitoring (RMON) alarm and event entries to monitor the value of a MIB object.

To configure RMON alarm and event entries, you include statements at the **[edit snmp]** hierarchy level of the configuration:

```
[edit snmp]
rmon {
  alarm index {
    description text-description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    rising-event-index index;
    rising-threshold integer;
    request-type (get-next-request | get-request | walk-request);
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
    syslog-subtag syslog-subtag;
    variable oid-variable;
    event index {
      community community-name;
      description description;
      type type;
    }
  }
}
```

- Related Documentation**
- [Understanding RMON Alarms on page 1621](#)
 - [Understanding RMON Events on page 1623](#)
 - [Configuring an Alarm Entry and Its Attributes on page 1626](#)
 - [Configuring an Event Entry and Its Attributes on page 1630](#)

Minimum RMON Alarm and Event Entry Configuration

To enable RMON on the router, you must configure an alarm entry and an event entry. To do this, include the following statements at the **[edit snmp rmon]** hierarchy level:

```
[edit snmp rmon]
alarm index {
  rising-event-index index;
  rising-threshold integer;
  sample-type type;
  variable oid-variable;
}
event index;
```

- Related Documentation**
- [Understanding RMON Alarms and Events Configuration on page 1625](#)
 - [Configuring an Alarm Entry and Its Attributes on page 1626](#)
 - [Configuring an Event Entry and Its Attributes on page 1630](#)

Configuring an Alarm Entry and Its Attributes

An alarm entry monitors the value of a MIB variable. You can configure how often the value is sampled, the type of sampling to perform, and what event to trigger if a threshold is crossed.

This section discusses the following topics:

- [Configuring the Alarm Entry on page 1627](#)
- [Configuring the Description on page 1627](#)
- [Configuring the Falling Event Index or Rising Event Index on page 1627](#)
- [Configuring the Falling Threshold or Rising Threshold on page 1627](#)
- [Configuring the Interval on page 1628](#)
- [Configuring the Falling Threshold Interval on page 1628](#)
- [Configuring the Request Type on page 1629](#)
- [Configuring the Sample Type on page 1629](#)
- [Configuring the Startup Alarm on page 1629](#)
- [Configuring the System Log Tag on page 1630](#)
- [Configuring the Variable on page 1630](#)

Configuring the Alarm Entry

An alarm entry monitors the value of a MIB variable. The **rising-event-index**, **rising-threshold**, **sample-type**, and **variable** statements are mandatory. All other statements are optional.

To configure the alarm entry, include the **alarm** statement and specify an index at the **[edit snmp rmon]** hierarchy level:

```
[edit snmp rmon]
alarm index {
  description description;
  falling-event-index index;
  falling-threshold integer;
  falling-threshold-interval seconds;
  interval seconds;
  rising-event-index index;
  rising-threshold integer;
  sample-type (absolute-value | delta-value);
  startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
  variable oid-variable;
}
```

index is an integer that identifies an alarm or event entry.

Configuring the Description

The description is a text string that identifies the alarm entry.

To configure the description, include the **description** statement and a description of the alarm entry at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
description description;
```

Configuring the Falling Event Index or Rising Event Index

The falling event index identifies the event entry that is triggered when a falling threshold is crossed. The rising event index identifies the event entry that is triggered when a rising threshold is crossed.

To configure the falling event index or rising event index, include the **falling-event-index** or **rising-event-index** statement and specify an index at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
falling-event-index index;
rising-event-index index;
```

index can be from 0 through 65,535. The default for both the falling and rising event index is 0.

Configuring the Falling Threshold or Rising Threshold

The falling threshold is the lower threshold for the monitored variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling

interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated startup alarm is equal to **falling-alarm** or **rising-or-falling-alarm**. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising threshold. You must specify the falling threshold as an integer. Its default is 20 percent less than the rising threshold.

By default, the rising threshold is 0. The rising threshold is the upper threshold for the monitored variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold, and the associated **startup-alarm** is equal to **rising-alarm** or **rising-or-falling-alarm**. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. You must specify the rising threshold as an integer.

To configure the falling threshold or rising threshold, include the **falling-threshold** or **rising-threshold** statement at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
  falling-threshold integer;
  rising-threshold integer;
```

integer can be a value from -2,147,483,647 through 2,147,483,647.

Configuring the Interval

The interval represents the period of time, in seconds, over which the monitored variable is sampled and compared with the rising and falling thresholds.

To configure the interval, include the **interval** statement and specify the number of seconds at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
  interval seconds;
```

seconds can be a value from 1 through 2,147,483,647. The default is 60 seconds.

Configuring the Falling Threshold Interval

The falling threshold interval represents the interval between samples when the rising threshold is crossed. Once the alarm crosses the falling threshold, the regular sampling interval is used.



NOTE: You cannot configure the falling threshold interval for alarms that have the request type set to **walk-request**.

To configure the falling threshold interval, include the **falling-threshold interval** statement at the **[edit snmp rmon alarm index]** hierarchy level and specify the number of seconds:

```
[edit snmp rmon alarm index]
  falling-threshold-interval seconds;
```

seconds can be a value from 1 through 2,147,483,647. The default is 60 seconds.

Configuring the Request Type

By default an RMON alarm can monitor only one object instance (as specified in the configuration). You can configure a **request-type** statement to extend the scope of the RMON alarm to include all object instances belonging to a MIB branch or to include the next object instance after the instance specified in the configuration.

To configure the request type, include the **request-type** statement at the **[edit snmp rmon alarm index]** hierarchy level and specify **get-next-request**, **get-request**, or **walk-request**:

```
[edit snmp rmon alarm index]
request-type (get-next-request | get-request | walk-request);
```

walk extends the RMON alarm configuration to all object instances belonging to a MIB branch. **next** extends the RMON alarm configuration to include the next object instance after the instance specified in the configuration.

Configuring the Sample Type

The sample type identifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is **absolute-value**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is **delta-value**, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.

To configure the sample type, include the **sample-type** statement and specify the type of sample at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
sample-type (absolute-value | delta-value);
```

- **absolute-value**—Actual value of the selected variable is compared against the thresholds.
- **delta-value**—Difference between samples of the selected variable is compared against the thresholds.

Configuring the Startup Alarm

The startup alarm identifies the type of alarm that can be sent when this entry is first activated. You can specify it as **falling-alarm**, **rising-alarm**, or **rising-or-falling-alarm**.

To configure the startup alarm, include the **startup-alarm** statement and specify the type of alarm at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

- **falling-alarm**—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.
- **rising-alarm**—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.

- **rising-or-falling-alarm**—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

The default is **rising-or-falling-alarm**.

Configuring the System Log Tag

The **syslog-subtag** statement specifies the tag to be added to the system log message. You can specify a string of not more than 80 uppercase characters as the system log tag.

To configure the system log tag, include the **syslog-subtag** statement at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
syslog-subtag syslog-subtag;
```

Configuring the Variable

The variable identifies the MIB object that is being monitored.

To configure the variable, include the **variable** statement and specify the object identifier or object name at the **[edit snmp rmon alarm index]** hierarchy level:

```
[edit snmp rmon alarm index]
variable oid-variable;
```

oid-variable is a dotted decimal (for example, 1.3.6.1.2.1.2.1.2.2.1.10.1) or MIB object name (for example, ifInOctets.1).

Configuring an Event Entry and Its Attributes

An event entry generates a notification for an alarm entry when its rising or falling threshold is crossed. You can configure the type of notification that is generated. To configure the event entry, include the **event** statement at the **[edit snmp rmon]** hierarchy level. All statements except the **event** statement are optional.

```
[edit snmp rmon]
event index {
  community community-name;
  description description;
  type type;
}
```

index identifies an entry event.

community-name is the trap group that is used when generating a trap. If that trap group has the **rmon-alarm** trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group. If nothing is configured, all the trap groups are examined, and traps are sent using each group with the **rmon-alarm** category set.

description is a text string that identifies the entry.

The **type** variable of an event entry specifies where the event is to be logged. You can specify the type as one of the following:

- **log**—Adds the event entry to the **logTable**.
- **log-and-trap**—Sends an SNMP trap and creates a log entry.
- **none**—Sends no notification.
- **snmptrap**—Sends an SNMP trap.

The default for the event entry type is **log-and-trap**.

**Related
Documentation**

- [Understanding RMON Alarms and Events Configuration on page 1625](#)
- [Understanding RMON Alarms on page 1621](#)
- [Understanding RMON Events on page 1623](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [Example: Configuring an RMON Alarm and Event Entry on page 1631](#)

Example: Configuring an RMON Alarm and Event Entry

Configure an RMON alarm and event entry:

```
[edit snmp]
rmon {
  alarm 100 {
    description "input traffic on fxp0";
    falling-event-index 100;
    falling-threshold 10000;
    interval 60;
    rising-event-index 100;
    rising-threshold 100000;
    sample-type delta-value;
    startup-alarm rising-or-falling-alarm;
    variable ifInOctets.1;
  }
  event 100 {
    community bedrock;
    description "emergency events";
    type log-and-trap;
  }
}
```

**Related
Documentation**

- [Understanding RMON Alarms and Events Configuration on page 1625](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [Configuring an Event Entry and Its Attributes on page 1630](#)

Monitoring RMON Alarms and Events

- [Using alarmTable to Monitor MIB Objects on page 1633](#)
- [Using eventTable to Log Alarms on page 1636](#)

Using alarmTable to Monitor MIB Objects

To use **alarmTable** to monitor a MIB object, perform the following tasks:

- [Creating an Alarm Entry on page 1633](#)
- [Configuring the Alarm MIB Objects on page 1633](#)
- [Activating a New Row in alarmTable on page 1636](#)
- [Modifying an Active Row in alarmTable on page 1636](#)
- [Deactivating a Row in alarmTable on page 1636](#)

Creating an Alarm Entry

To create an alarm entry, first create a new row in **alarmTable** using the **alarmStatus** object. For example, create alarm #1 using the UCD command-line utilities:

```
snmpset -Os -v2c router community alarmStatus.1 i createRequest
```

Configuring the Alarm MIB Objects

Once you have created the new row in **alarmTable**, configure the following Alarm MIB objects:



NOTE: Other than **alarmStatus**, you cannot modify any of the objects in the entry if the associated **alarmStatus** object is set to valid.

- [alarmInterval on page 1634](#)
- [alarmVariable on page 1634](#)
- [alarmSampleType on page 1634](#)
- [alarmValue on page 1634](#)
- [alarmStartupAlarm on page 1634](#)
- [alarmRisingThreshold on page 1635](#)

- [alarmFallingThreshold](#) on page 1635
- [alarmOwner](#) on page 1635
- [alarmRisingEventIndex](#) on page 1635
- [alarmFallingEventIndex](#) on page 1635

alarmInterval

The interval, in seconds, over which data is sampled and compared with the rising and falling thresholds. For example, to set **alarmInterval** for alarm #1 to 30 seconds, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmInterval.1 i 30
```

alarmVariable

The object identifier of the variable to be sampled. During a **Set** request, if the supplied variable name is not available in the selected MIB view, a **badValue** error is returned. If at any time the variable name of an established **alarmEntry** is no longer available in the selected MIB view, the probe changes the status of **alarmVariable** to invalid. For example, to identify **ifInOctets.61** as the variable to be monitored, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmVariable.1 o .1.3.6.1.2.1.2.2.1.10.61
```

alarmSampleType

The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is **absoluteValue**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is **deltaValue**, the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds. For example, to set **alarmSampleType** for alarm #1 to **deltaValue**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmSampleType.1 i deltaValue
```

alarmValue

The value of the variable during the last sampling period. This value is compared with the rising and falling thresholds. If the sample type is **deltaValue**, this value equals the difference between the samples at the beginning and end of the period. If the sample type is **absoluteValue**, this value equals the sampled value at the end of the period.

alarmStartupAlarm

An alarm that is sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to **risingThreshold**, and **alarmStartupAlarm** is equal to **risingAlarm** or **risingOrFallingAlarm**, then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to **fallingThreshold** and **alarmStartupAlarm** is equal to **fallingAlarm** or **risingOrFallingAlarm**, then a single falling

alarm is generated. For example, to set **alarmStartupAlarm** for alarm #1 to **risingOrFallingAlarm**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStartupAlarm.1 i risingOrFallingAlarm
```

alarmRisingThreshold

A threshold for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold, and the associated **alarmStartupAlarm** is equal to **risingAlarm** or **risingOrFallingAlarm**. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches **alarmFallingThreshold**. For example, to set **alarmRisingThreshold** for alarm #1 to **100000**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmRisingThreshold.1 i 100000
```

alarmFallingThreshold

A threshold for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated **alarmStartupAlarm** is equal to **fallingAlarm** or **risingOrFallingAlarm**. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches **alarmRisingThreshold**. For example, to set **alarmFallingThreshold** for alarm #1 to **10000**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 10000
```

alarmOwner

Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.

alarmRisingEventIndex

The index of the **eventEntry** object that is used when a rising threshold is crossed. If there is no corresponding entry in **eventTable**, then no association exists. If this value is zero, no associated event is generated because zero is not a valid event index. For example, to set **alarmRisingEventIndex** for alarm #1 to **10**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmRisingEventIndex.1 i 10
```

alarmFallingEventIndex

The index of the **eventEntry** object that is used when a falling threshold is crossed. If there is no corresponding entry in **eventTable**, then no association exists. If this value is zero, no associated event is generated because zero is not a valid event index. For example, to set **alarmFallingEventIndex** for alarm #1 to **10**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingEventIndex.1 i 10
```

Activating a New Row in alarmTable

To activate a new row in **alarmTable**, set **alarmStatus** to **valid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Modifying an Active Row in alarmTable

To modify an active row, first set **alarmStatus** to **underCreation** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i underCreation
```

Then change the row contents using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 1000
```

Finally, activate the row by setting **alarmStatus** to **valid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Deactivating a Row in alarmTable

To deactivate a row in **alarmTable**, set **alarmStatus** to **invalid** using an SNMP **Set** request:

```
snmpset -Os -v2c router community alarmStatus.1 i invalid
```

Related Documentation

- [Understanding RMON Alarms on page 1621](#)
- [Understanding RMON Events on page 1623](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)

Using eventTable to Log Alarms

To use **eventTable** to log alarms, perform the following tasks:

- [Creating an Event Entry on page 1636](#)
- [Configuring the MIB Objects on page 1637](#)
- [Activating a New Row in eventTable on page 1638](#)
- [Deactivating a Row in eventTable on page 1638](#)

Creating an Event Entry

The RMON **eventTable** controls the generation of notifications from the router. Notifications can be logs (entries to **logTable** and **syslogs**) or SNMP traps. Each event entry can be configured to generate any combination of these notifications (or no notification). When an event specifies that an SNMP trap is to be generated, the trap group that is used when sending the trap is specified by the value of the associated **eventCommunity** object. Consequently, the community in the trap message will match the value specified by **eventCommunity**. If nothing is configured for **eventCommunity**, a trap is sent using each trap group that has the **rmon-alarm** category configured.

Configuring the MIB Objects

Once you have created the new row in **eventTable**, set the following objects:



NOTE: The **eventType** object is required. All other objects are optional.

- [eventType](#) on page 1637
- [eventCommunity](#) on page 1637
- [eventOwner](#) on page 1637
- [eventDescription](#) on page 1638

eventType

The type of notification that the router generates when the event is triggered.

This object can be set to the following values:

- **log**—Adds the event entry to **logTable**.
- **log-and-trap**—Sends an SNMP trap and creates a log entry.
- **none**—Sends no notification.
- **snmptrap**—Sends an SNMP trap.

For example, to set **eventType** for event #1 to **log-and-trap**, use the following SNMP Set request:

```
snmpset -Os -v2c router community eventType.1 i log-and-trap
```

eventCommunity

The trap group that is used when generating a trap (if **eventType** is configured to send traps). If that trap group has the **rmon-alarm** trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of **eventCommunity**). If nothing is configured, traps are sent to each group with the **rmon-alarm** category set. For example, to set **eventCommunity** for event #1 to **boy-elroy**, use the following SNMP Set request:

```
snmpset -Os -v2c router community eventCommunity.1 s "boy-elroy"
```



NOTE: The **eventCommunity** object is optional. If you do not set this object, then the field is left blank.

eventOwner

Any text string specified by the creating management application or the command-line interface (CLI). Typically, it is used to identify a network manager (or application) and can be used for fine access control between participating management applications.

For example, to set **eventOwner** for event #1 to **george jetson**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventOwner.1 s "george jetson"
```



NOTE: The **eventOwner** object is optional. If you do not set this object, then the field is left blank.

eventDescription

Any text string specified by the creating management application or the command-line interface (CLI). The use of this string is application dependent.

For example, to set **eventDescription** for event #1 to **spacelys sprockets**, use the following SNMP **Set** request:

```
snmpset -Os -v2c router community eventDescription.1 s "spacelys sprockets"
```



NOTE: The **eventDescription** object is optional. If you do not set this object, then the field is left blank.

Activating a New Row in eventTable

To activate the new row in **eventTable**, set **eventStatus** to **valid** using an SNMP **Set** request such as:

```
snmpset -Os -v2c router community eventStatus.1 i valid
```

Deactivating a Row in eventTable

To deactivate a row in **eventTable**, set **eventStatus** to **invalid** using an SNMP **Set** request such as:

```
snmpset -Os -v2c router community eventStatus.1 i invalid
```

Related Documentation

- [Understanding RMON Alarms on page 1621](#)
- [Understanding RMON Events on page 1623](#)
- [Configuring an Event Entry and Its Attributes on page 1630](#)

CHAPTER 72

Using RMON to Monitor Network Service Quality

- [Understanding RMON for Monitoring Service Quality on page 1639](#)
- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)
- [Defining and Measuring Network Availability on page 1644](#)
- [Measuring Health on page 1650](#)
- [Measuring Performance on page 1656](#)

Understanding RMON for Monitoring Service Quality

Health and performance monitoring can benefit from the remote monitoring of SNMP variables by the local SNMP agents running on each router. The SNMP agents compare MIB values against predefined thresholds and generate exception alarms without the need for polling by a central SNMP management platform. This is an effective mechanism for proactive management, as long as the thresholds have baselines determined and set correctly. For more information, see RFC 2819, *Remote Network Monitoring MIB*.

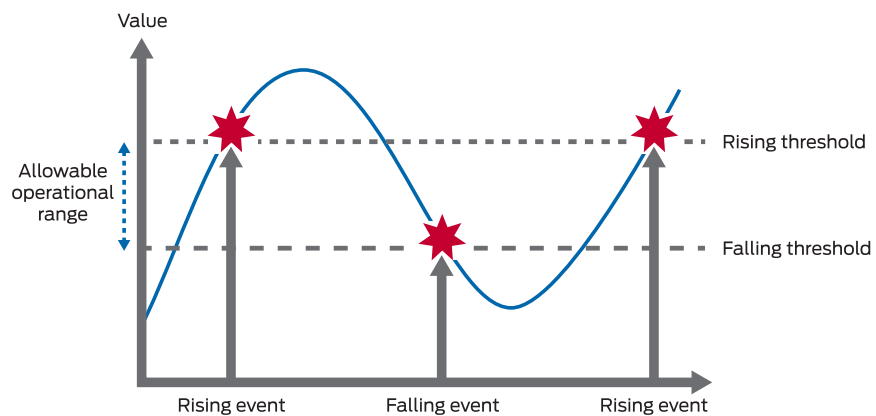
This topic includes the following sections:

- [Setting Thresholds on page 1639](#)
- [RMON Command-Line Interface on page 1640](#)
- [RMON Event Table on page 1641](#)
- [RMON Alarm Table on page 1641](#)
- [Troubleshooting RMON on page 1642](#)

Setting Thresholds

By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside of the allowable operational range. (See [Figure 35](#).)

Figure 35: Setting Thresholds



g041661

Events are only generated when the threshold is first crossed in any one direction rather than after each sample period. For example, if a rising threshold crossing event is raised, no more threshold crossing events will occur until a corresponding falling event. This considerably reduces the quantity of alarms that are produced by the system, making it easier for operations staff to react when alarms do occur.

To configure remote monitoring, specify the following pieces of information:

- The variable to be monitored (by its SNMP object identifier)
- The length of time between each inspection
- A rising threshold
- A falling threshold
- A rising event
- A falling event

Before you can successfully configure remote monitoring, you should identify what variables need to be monitored and their allowable operational range. This requires some period of baselining to determine the allowable operational ranges. An initial baseline period of at least three months is not unusual when first identifying the operational ranges and defining thresholds, but baseline monitoring should continue over the life span of each monitored variable.

RMON Command-Line Interface

Junos OS provides two mechanisms you use to control the Remote Monitoring agent on the router: command-line interface (CLI) and SNMP. To configure an RMON entry using the CLI, include the following statements at the **[edit snmp]** hierarchy level:

```
rmon {
  alarm index {
    description;
    falling-event-index;
    falling-threshold;
    intervals;
    rising-event-index;
```



```

    rising-threshold;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling | rising | rising-or-falling);
    variable;
  }
  event index {
    community;
    description;
    type (log | trap | log-and-trap | none);
  }
}

```

If you do not have CLI access, you can configure remote monitoring using the SNMP Manager or management application, assuming SNMP access has been granted. (See [Table 125](#).) To configure RMON using SNMP, perform SNMP **Set** requests to the RMON event and alarm tables.

RMON Event Table

Set up an event for each type that you want to generate. For example, you could have two generic events, *rising* and *falling*, or many different events for each variable that is being monitored (for example, *temperature rising* event, *temperature falling* event, *firewall hit* event, *interface utilization* event, and so on). Once the events have been configured, you do not need to update them.

Table 125: RMON Event Table

Field	Description
eventDescription	Text description of this event
eventType	Type of event (for example, log , trap , or log and trap)
eventCommunity	Trap group to which to send this event (as defined in the Junos OS configuration, which is not the same as the community)
eventOwner	Entity (for example, manager) that created this event
eventStatus	Status of this row (for example, valid , invalid , or createRequest)

RMON Alarm Table

The RMON alarm table stores the SNMP object identifiers (including their instances) of the variables that are being monitored, together with any rising and falling thresholds and their corresponding event indexes. To create an RMON request, specify the fields shown in [Table 126](#).

Table 126: RMON Alarm Table

Field	Description
alarmStatus	Status of this row (for example, valid , invalid , or createRequest)

Table 126: RMON Alarm Table (*continued*)

Field	Description
alarmInterval	Sampling period (in seconds) of the monitored variable
alarmVariable	OID (and instance) of the variable to be monitored
alarmValue	Actual value of the sampled variable
alarmSampleType	Sample type (absolute or delta changes)
alarmStartupAlarm	Initial alarm (rising , falling , or either)
alarmRisingThreshold	Rising threshold against which to compare the value
alarmFallingThreshold	Falling threshold against which to compare the value
alarmRisingEventIndex	Index (row) of the rising event in the event table
alarmFallingEventIndex	Index (row) of the falling event in the event table

Both the **alarmStatus** and **eventStatus** fields are **entryStatus** primitives, as defined in RFC 2579, *Textual Conventions for SMIV2*.

Troubleshooting RMON

You troubleshoot the RMON agent, **rmopd**, that runs on the router by inspecting the contents of the Juniper Networks enterprise RMON MIB, **jnxRmon**, which provides the extensions listed in [Table 127](#) to the RFC 2819 **alarmTable**.

Table 127: jnxRmon Alarm Extensions

Field	Description
jnxRmonAlarmGetFailCnt	Number of times the internal Get request for the variable failed
jnxRmonAlarmGetFailTime	Value of sysUpTime when the last failure occurred
jnxRmonAlarmGetFailReason	Reason why the Get request failed
jnxRmonAlarmGetOkTime	Value of sysUpTime when the variable moved out of failure state
jnxRmonAlarmState	Status of this alarm entry

Monitoring the extensions in this table provides clues as to why remote alarms may not behave as expected.

Related Documentation

- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)

Understanding Measurement Points, Key Performance Indicators, and Baseline Values

This chapter topic provides guidelines for monitoring the service quality of an IP network. It describes how service providers and network administrators can use information provided by Juniper Networks routers to monitor network performance and capacity. You should have a thorough understanding of the SNMP and the associated MIB supported by Junos OS.



NOTE: For a good introduction to the process of monitoring an IP network, see RFC 2330, *Framework for IP Performance Metrics*.

This topic contains the following sections:

- [Measurement Points on page 1643](#)
- [Basic Key Performance Indicators on page 1644](#)
- [Setting Baselines on page 1644](#)

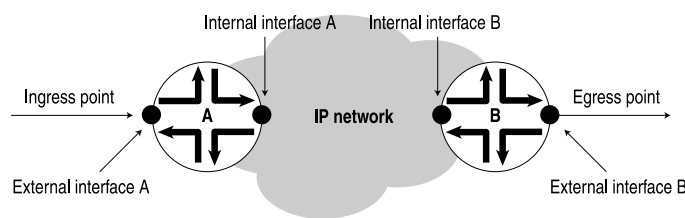
Measurement Points

Defining the measurement points where metrics are measured is equally as important as defining the metrics themselves. This section describes measurement points within the context of this chapter and helps identify where measurements can be taken from a service provider network. It is important to understand exactly where a measurement point is. Measurement points are vital to understanding the implication of what the actual measurement means.

An IP network consists of a collection of routers connected by physical links that are all running the Internet Protocol. You can view the network as a collection of routers with an ingress (entry) point and an egress (exit) point. See [Figure 36](#).

- Network-centric measurements are taken at measurement points that most closely map to the ingress and egress points for the network itself. For example, to measure delay across the provider network from Site A to Site B, the measurement points should be the ingress point to the provider network at Site A and the egress point at Site B.
- Router-centric measurements are taken directly from the routers themselves, but be careful to ensure that the correct router subcomponents have been identified in advance.

Figure 36: Network Entry Points



9017042



NOTE: [Figure 36](#) does not show the client networks at customer premises, but they would be located on either side of the ingress and egress points. Although this chapter does not discuss how to measure network services as perceived by these client networks, you can use measurements taken for the service provider network as input into such calculations.

Basic Key Performance Indicators

For example, you could monitor a service provider network for three basic key performance indicators (KPIs):

- *Availability* measures the “reachability” of one measurement point from another measurement point at the network layer (for example, using ICMP ping). The underlying routing and transport infrastructure of the provider network will support the availability measurements, with failures highlighted as unavailability.
- *Health* measures the number and type of errors that are occurring on the provider network, and can consist of both router-centric and network-centric measurements, such as hardware failures or packet loss.
- *Performance* of the provider network measures how well it can support IP services (for example, in terms of delay or utilization).

Setting Baselines

How well is the provider network performing? We recommend an initial three-month period of monitoring to identify a network’s normal operational parameters. With this information, you can recognize exceptions and identify abnormal behavior. You should continue baseline monitoring for the lifetime of each measured metric. Over time, you must be able to recognize performance trends and growth patterns.

Within the context of this chapter, many of the metrics identified do not have an allowable operational range associated with them. In most cases, you cannot identify the allowable operational range until you have determined a baseline for the actual variable on a specific network.

Related Documentation

- [Understanding RMON for Monitoring Service Quality on page 1639](#)
- [Defining and Measuring Network Availability on page 1644](#)
- [Measuring Health on page 1650](#)
- [Measuring Performance on page 1656](#)

Defining and Measuring Network Availability

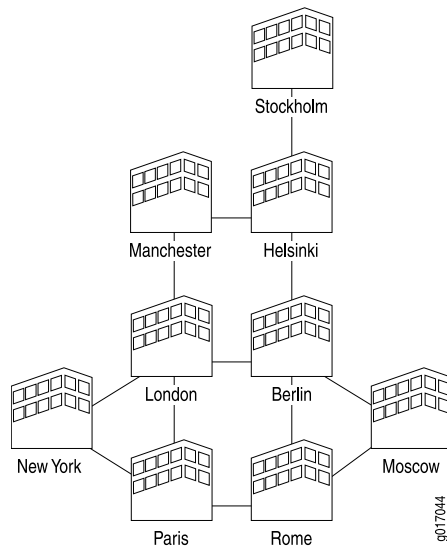
This topic includes the following sections:

- [Defining Network Availability on page 1645](#)
- [Measuring Availability on page 1647](#)

Defining Network Availability

Availability of a service provider's IP network can be thought of as the reachability between the regional points of presence (POP), as shown in [Figure 37](#).

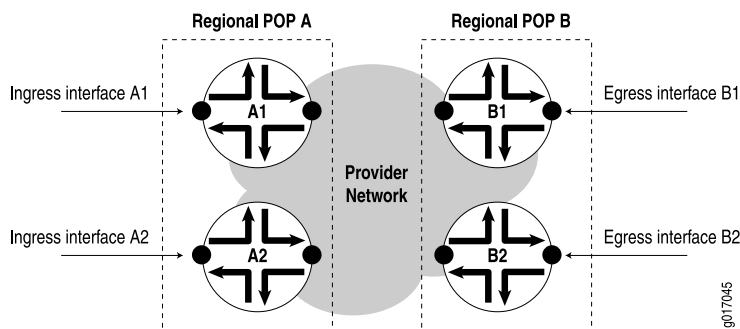
Figure 37: Regional Points of Presence



With the example above, when you use a full mesh of measurement points, where every POP measures the availability to every other POP, you can calculate the total availability of the service provider's network. This KPI can also be used to help monitor the service level of the network, and can be used by the service provider and its customers to determine if they are operating within the terms of their service-level agreement (SLA).

Where a POP may consist of multiple routers, take measurements to each router as shown in [Figure 38](#).

Figure 38: Measurements to Each Router



Measurements include:

- Path availability—Availability of an egress interface **B1** as seen from an ingress interface **A1**.
- Router availability—Percentage of path availability of all measured paths terminating on the router.
- POP availability—Percentage of router availability between any two regional POPs, **A** and **B**.
- Network availability—Percentage of POP availability for all regional POPs in the service provider's network.

To measure POP availability of **POP A** to **POP B** in [Figure 38](#), you must measure the following four paths:

Path A1 => B1
Path A1 => B2
Path A2 => B1
Path A2 => B2

Measuring availability from **POP B** to **POP A** would require a further four measurements, and so on.

A full mesh of availability measurements can generate significant management traffic. From the sample diagram above:

- Each POP has two co-located provider edge (PE) routers, each with 2xSTM1 interfaces, for a total of 18 PE routers and 36xSTM1 interfaces.
- There are six core provider (P) routers, four with 2xSTM4 and 3xSTM1 interfaces each, and two with 3xSTM4 and 3xSTM1 interfaces each.

This makes a total of 68 interfaces. A full mesh of paths between every interface is:

$[n \times (n-1)] / 2$ gives $[68 \times (68-1)] / 2 = 2278$ paths

To reduce management traffic on the service provider's network, instead of generating a full mesh of interface availability tests (for example, from each interface to every other interface), you can measure from each router's loopback address. This reduces the number of availability measurements required to a total of one for each router, or:

$[n \times (n-1)] / 2$ gives $[24 \times (24-1)] / 2 = 276$ measurements

This measures availability from each router to every other router.

Monitoring the SLA and the Required Bandwidth

A typical SLA between a service provider and a customer might state:

A Point of Presence is the connection of two back-to-back provider edge routers to separate core provider routers using different links for resilience. The system is considered to be unavailable when either an entire POP becomes unavailable or for the duration of a Priority 1 fault.

An SLA availability figure of 99.999 percent for a provider's network would relate to a down time of approximately 5 minutes per year. Therefore, to measure this proactively,

you would have to take availability measurements at a granularity of less than one every five minutes. With a standard size of 64 bytes per ICMP ping request, one ping test per minute would generate 7680 bytes of traffic per hour per destination, including ping responses. A full mesh of ping tests to 276 destinations would generate 2,119,680 bytes per hour, which represents the following:

- On an OC3/STM1 link of 155.52 Mbps, a utilization of 1.362 percent
- On an OC12/STM4 link of 622.08 Mbps, a utilization of 0.340 percent

With a size of 1500 bytes per ICMP ping request, one ping test per minute would generate 180,000 bytes per hour per destination, including ping responses. A full mesh of ping tests to 276 destinations would generate 49,680,000 bytes per hour, which represents the following:

- On an OC3/STM1 link, 31.94 percent utilization
- On an OC12/STM4 link, 7.986 percent utilization

Each router can record the results for every destination tested. With one test per minute to each destination, a total of $1 \times 60 \times 24 \times 276 = 397,440$ tests per day would be performed and recorded by each router. All ping results are stored in the **pingProbeHistoryTable** (see RFC 2925) and can be retrieved by an SNMP performance reporting application (for example, service performance management software from InfoVista, Inc., or Concord Communications, Inc.) for post processing. This table has a maximum size of 4,294,967,295 rows, which is more than adequate.

Measuring Availability

There are two methods you can use to measure availability:

- Proactive—Availability is automatically measured as often as possible by an operational support system.
- Reactive—Availability is recorded by a Help desk when a fault is first reported by a user or a fault monitoring system.

This section discusses real-time performance monitoring as a proactive monitoring solution.

Real-Time Performance Monitoring

Juniper Networks provides a real-time performance monitoring (RPM) service to monitor real-time network performance. Use the J-Web Quick Configuration feature to configure real-time performance monitoring parameters used in real-time performance monitoring tests. (J-Web Quick Configuration is a browser-based GUI that runs on Juniper Networks routers. For more information, see the *J-Web Interface User Guide*.)

Configuring Real-Time Performance Monitoring

Some of the most common options you can configure for real-time performance monitoring tests are shown in [Table 128](#).

Table 128: Real-Time Performance Monitoring Configuration Options

Field	Description
Request Information	
Probe Type	Type of probe to send as part of the test. Probe types can be: <ul style="list-style-type: none"> • http-get • http-get-metadata • icmp-ping • icmp-ping-timestamp • tcp-ping • udp-ping
Interval	Wait time (in seconds) between each probe transmission. The range is 1 to 255 seconds.
Test Interval	Wait time (in seconds) between tests. The range is 0 to 86400 seconds.
Probe Count	Total number of probes sent for each test. The range is 1 to 15 probes.
Destination Port	TCP or UDP port to which probes are sent. Use number 7—a standard TCP or UDP port number—or select a port number from 49152 through 65535.
DSCP Bits	Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is 000000.
Data Size	Size (in bytes) of the data portion of the ICMP probes. The range is 0 to 65507 bytes.
Data Fill	Contents of the data portion of the ICMP probes. Contents must be a hexadecimal value. The range is 1 to 800h.
Maximum Probe Thresholds	
Successive Lost Probes	Total number of probes that must be lost successively to trigger a probe failure and generate a system log message. The range is 0 to 15 probes.
Lost Probes	Total number of probes that must be lost to trigger a probe failure and generate a system log message. The range is 0 to 15 probes.
Round Trip Time	Total round-trip time (in microseconds) from the Services Router to the remote server, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Jitter	Total jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.

Table 128: Real-Time Performance Monitoring Configuration Options (*continued*)

Field	Description
Standard Deviation	Maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Egress Time	Total one-way time (in microseconds) from the router to the remote server, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Ingress Time	Total one-way time (in microseconds) from the remote server to the router, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Jitter Egress Time	Total outbound-time jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Jitter Ingress Time	Total inbound-time jitter (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Egress Standard Deviation	Maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.
Ingress Standard Deviation	Maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. The range is 0 to 60,000,000 microseconds.

Displaying Real-Time Performance Monitoring Information

For each real-time performance monitoring test configured on the router, monitoring information includes the round-trip time, jitter, and standard deviation. To view this information, select **Monitor > RPM** in the J-Web interface, or enter the **show services rpm** command-line interface (CLI) command.

To display the results of the most recent real-time performance monitoring probes, enter the **show services rpm probe-results** CLI command:

```

user@host> show services rpm probe-results
Owner: p1, Test: t1
Target address: 10.8.4.1, Source address: 10.8.4.2, Probe type: icmp-ping
Destination interface name: lt-0/0/0.0
Test size: 10 probes
Probe results:
  Response received, Sun Jul 10 19:07:34 2005
  Rtt: 50302 usec
Results over current test:
```

```

Probes sent: 2, Probes received: 1, Loss percentage: 50
Measurement: Round trip time
  Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
  Jitter: 0 usec, Stddev: 0 usec
Results over all tests:
Probes sent: 2, Probes received: 1, Loss percentage: 50
Measurement: Round trip time
  Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
  Jitter: 0 usec, Stddev: 0 usec

```

- Related Documentation**
- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)
 - [Understanding RMON for Monitoring Service Quality on page 1639](#)
 - [Measuring Health on page 1650](#)
 - [Measuring Performance on page 1656](#)

Measuring Health

You can monitor health metrics reactively by using fault management software such as SMARTS InCharge, Micromuse Netcool Omnibus, or Concord Live Exceptions. We recommend that you monitor the health metrics shown in [Table 129](#).

Table 129: Health Metrics

Metric:	Errors in
Description	Number of inbound packets that contained errors, preventing them from being delivered
MIB name	IF-MIB (RFC 2233)
Variable name	ifInErrors
Variable OID	.1.3.6.1.31.2.2.1.14
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	Logical interfaces
Metric:	Errors out
Description	Number of outbound packets that contained errors, preventing them from being transmitted
MIB name	IF-MIB (RFC 2233)
Variable name	ifOutErrors

Table 129: Health Metrics (*continued*)

Variable OID	.1.3.6.1.31.2.2.1.20
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	Logical interfaces
Metric:	Discards in
Description	Number of inbound packets discarded, even though no errors were detected
MIB name	IF-MIB (RFC 2233)
Variable name	ifInDiscards
Variable OID	.1.3.6.1.31.2.2.1.13
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	Logical interfaces
Metric:	Unknown protocols
Description	Number of inbound packets discarded because they were of an unknown protocol
MIB name	IF-MIB (RFC 2233)
Variable name	ifInUnknownProtos
Variable OID	.1.3.6.1.31.2.2.1.15
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	Logical interfaces
Metric:	Interface operating status
Description	Operational status of an interface
MIB name	IF-MIB (RFC 2233)
Variable name	ifOperStatus

Table 129: Health Metrics (*continued*)

Variable OID	.1.3.6.1.31.2.2.1.8
Frequency (mins)	15
Allowable range	1 (up)
Managed objects	Logical interfaces
Metric:	Label Switched Path (LSP) state
Description	Operational state of an MPLS label-switched path
MIB name	MPLS-MIB
Variable name	mplsLspState
Variable OID	mplsLspEntry.2
Frequency (mins)	60
Allowable range	2 (up)
Managed objects	All label-switched paths in the network
Metric:	Component operating status
Description	Operational status of a router hardware component
MIB name	JUNIPER-MIB
Variable name	jnxOperatingState
Variable OID	.1.3.6.1.4.1.2636.1.13.1.6
Frequency (mins)	60
Allowable range	2 (running) or 3 (ready)
Managed objects	All components in each Juniper Networks router
Metric:	Component operating temperature
Description	Operational temperature of a hardware component, in Celsius
MIB name	JUNIPER-MIB
Variable name	jnxOperatingTemp
Variable OID	.1.3.6.1.4.1.2636.1.13.1.7

Table 129: Health Metrics (*continued*)

Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All components in a chassis
Metric:	System up time
Description	Time, in milliseconds, that the system has been operational.
MIB name	MIB-2 (RFC 1213)
Variable name	sysUpTime
Variable OID	.1.3.6.1.1.3
Frequency (mins)	60
Allowable range	Increasing only (decrement indicates a restart)
Managed objects	All routers
Metric:	No IP route errors
Description	Number of packets that could not be delivered because there was no IP route to their destination.
MIB name	MIB-2 (RFC 1213)
Variable name	ipOutNoRoutes
Variable OID	ip.12
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	Each router
Metric:	Wrong SNMP community names
Description	Number of incorrect SNMP community names received
MIB name	MIB-2 (RFC 1213)
Variable name	snmpInBadCommunityNames
Variable OID	snmp.4

Table 129: Health Metrics (*continued*)

Frequency (hours)	24
Allowable range	To be baselined
Managed objects	Each router
Metric:	SNMP community violations
Description	Number of valid SNMP communities used to attempt invalid operations (for example, attempting to perform SNMP Set requests)
MIB name	MIB-2 (RFC 1213)
Variable name	snmpInBadCommunityUses
Variable OID	snmp.5
Frequency (hours)	24
Allowable range	To be baselined
Managed objects	Each router
Metric:	Redundancy switchover
Description	Total number of redundancy switchovers reported by this entity
MIB name	JUNIPER-MIB
Variable name	jnxRedundancySwitchoverCount
Variable OID	jnxRedundancyEntry.8
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All Juniper Networks routers with redundant Routing Engines
Metric:	FRU state
Description	Operational status of each field-replaceable unit (FRU)
MIB name	JUNIPER-MIB
Variable name	jnxFruState
Variable OID	jnxFruEntry.8

Table 129: Health Metrics (*continued*)

Frequency (mins)	15
Allowable range	2 through 6 for ready/online states. See jnxFruOfflineReason in the event of a FRU failure.
Managed objects	All FRUs in all Juniper Networks routers.
Metric:	Rate of tail-dropped packets
Description	Rate of tail-dropped packets per output queue, per forwarding class, per interface.
MIB name	JUNIPER-COS-MIB
Variable name	jnxCosIfqTailDropPktRate
Variable OID	jnxCosIfqStatsEntry.12
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	For each forwarding class per interface in the provider network, when CoS is enabled.
Metric:	Interface utilization: octets received
Description	Total number of octets received on the interface, including framing characters.
MIB name	IF-MIB
Variable name	ifInOctets
Variable OID	.1.3.6.1.2.1.2.2.1.10.x
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All operational interfaces in the network
Metric:	Interface utilization: octets transmitted
Description	Total number of octets transmitted out of the interface, including framing characters.
MIB name	IF-MIB
Variable name	ifOutOctets

Table 129: Health Metrics (*continued*)

Variable OID	.1.3.6.1.2.1.2.2.1.16.x
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All operational interfaces in the network



NOTE: Byte counts vary depending on interface type, encapsulation used and PIC supported. For example, with vlan-ccc encapsulation on a 4xFE, GE, or GE IQ PIC, the byte count includes framing and control word overhead. (See [Table 130](#).)

Table 130: Counter Values for vlan-ccc Encapsulation

PIC Type	Encapsulation	Input (Unit Level)	Output (Unit Level)	SNMP
4xFE	vlan-ccc	Frame (no frame check sequence [FCS])	Frame (including FCS and control word)	ifInOctets, ifOutOctets
GE	vlan-ccc	Frame (no FCS)	Frame (including FCS and control word)	ifInOctets, ifOutOctets
GE IQ	vlan-ccc	Frame (no FCS)	Frame (including FCS and control word)	ifInOctets, ifOutOctets

SNMP traps are also a good mechanism to use for health management. For more information, see “[Standard SNMP Traps Supported on Devices Running Junos OS](#)” on [page 1456](#) and “[Juniper Networks Enterprise-Specific SNMP Traps](#)” on [page 1456](#) in the *SNMP MIBs and Traps Reference*.

Related Documentation

- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)
- [Understanding RMON for Monitoring Service Quality on page 1639](#)
- [Defining and Measuring Network Availability on page 1644](#)
- [Measuring Performance on page 1656](#)

Measuring Performance

The performance of a service provider's network is usually defined as how well it can support services, and is measured with metrics such as delay and utilization. We suggest that you monitor the following performance metrics using applications such as InfoVista Service Performance Management or Concord Network Health (see [Table 131](#)).

Table 131: Performance Metrics

Metric:	Average delay
Description	Average round-trip time (in milliseconds) between two measurement points.
MIB name	DISMAN-PING-MIB (RFC 2925)
Variable name	pingResultsAverageRtt
Variable OID	pingResultsEntry.6
Frequency (mins)	15 (or depending upon ping test frequency)
Allowable range	To be baselined
Managed objects	Each measured path in the network
Metric:	Interface utilization
Description	Utilization percentage of a logical connection.
MIB name	IF-MIB
Variable name	(ifInOctets & ifOutOctets) * 8 / ifSpeed
Variable OID	ifTable entries
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All operational interfaces in the network
Metric:	Disk utilization
Description	Utilization of disk space within the Juniper Networks router
MIB name	HOST-RESOURCES-MIB (RFC 2790)
Variable name	hrStorageSize – hrStorageUsed
Variable OID	hrStorageEntry.5 – hrStorageEntry.6
Frequency (mins)	1440
Allowable range	To be baselined
Managed objects	All Routing Engine hard disks

Table 131: Performance Metrics (*continued*)

Metric:	Memory utilization
Description	Utilization of memory on the Routing Engine and FPC.
MIB name	JUNIPER-MIB (Juniper Networks enterprise Chassis MIB)
Variable name	jnxOperatingHeap
Variable OID	Table for each component
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All Juniper Networks routers
Metric:	CPU load
Description	Average utilization over the past minute of a CPU.
MIB name	JUNIPER-MIB (Juniper Networks enterprise Chassis MIB)
Variable name	jnxOperatingCPU
Variable OID	Table for each component
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All Juniper Networks routers
Metric:	LSP utilization
Description	Utilization of the MPLS label-switched path.
MIB name	MPLS-MIB
Variable name	mplsPathBandwidth / (mplsLspOctets * 8)
Variable OID	mplsLspEntry.21 and mplsLspEntry.3
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	All label-switched paths in the network
Metric:	Output queue size

Table 131: Performance Metrics (*continued*)

Description	Size, in packets, of each output queue per forwarding class, per interface.
MIB name	JUNIPER-COS-MIB
Variable name	jnxCosIfqQedPkts
Variable OID	jnxCosIfqStatsEntry.3
Frequency (mins)	60
Allowable range	To be baselined
Managed objects	For each forwarding class per interface in the network, once CoS is enabled.

This section includes the following topics:

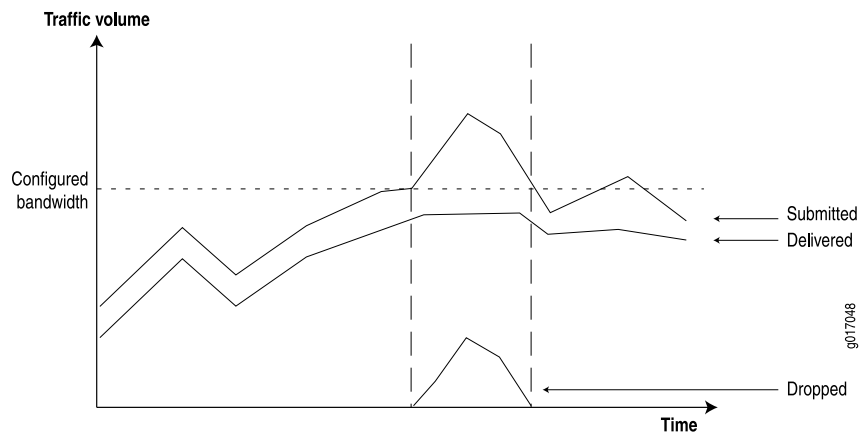
- [Measuring Class of Service on page 1659](#)
- [Inbound Firewall Filter Counters per Class on page 1660](#)
- [Monitoring Output Bytes per Queue on page 1661](#)
- [Dropped Traffic on page 1662](#)

Measuring Class of Service

You can use class-of-service (CoS) mechanisms to regulate how certain classes of packets are handled within your network during times of peak congestion. Typically you must perform the following steps when implementing a CoS mechanism:

- Identify the type of packets that is applied to this class. For example, include all customer traffic from a specific ingress edge interface within one class, or include all packets of a particular protocol such as voice over IP (VoIP).
- Identify the required deterministic behavior for each class. For example, if VoIP is important, give VoIP traffic the highest priority during times of network congestion. Conversely, you can downgrade the importance of Web traffic during congestion, as it may not impact customers too much.

With this information, you can configure mechanisms at the network ingress to monitor, mark, and police traffic classes. Marked traffic can then be handled in a more deterministic way at egress interfaces, typically by applying different queuing mechanisms for each class during times of network congestion. You can collect information from the network to provide customers with reports showing how the network is behaving during times of congestion. (See [Figure 39](#).)

Figure 39: Network Behavior During Congestion

To generate these reports, routers must provide the following information:

- Submitted traffic—Amount of traffic received per class.
- Delivered traffic—Amount of traffic transmitted per class.
- Dropped traffic—Amount of traffic dropped because of CoS limits.

The following section outlines how this information is provided by Juniper Networks routers.

Inbound Firewall Filter Counters per Class

Firewall filter counters are a very flexible mechanism you can use to match and count inbound traffic per class, per interface. For example:

```
firewall {
  filter f1 {
    term t1 {
      from {
        dscp af11;
      }
      then {
        # Assured forwarding class 1 drop profile 1 count inbound-af11;
        accept;
      }
    }
  }
}
```

For example, [Table 132](#) shows additional filters used to match the other classes.

Table 132: Inbound Traffic Per Class

DSCP Value	Firewall Match Condition	Description
10	af11	Assured forwarding class 1 drop profile 1
12	af12	Assured forwarding class 1 drop profile 2

Table 132: Inbound Traffic Per Class (*continued*)

DSCP Value	Firewall Match Condition	Description
18	af21	Best effort class 2 drop profile 1
20	af22	Best effort class 2 drop profile 2
26	af31	Best effort class 3 drop profile 1

Any packet with a CoS DiffServ code point (DSCP) conforming to RFC 2474 can be counted in this way. The Juniper Networks enterprise-specific Firewall Filter MIB presents the counter information in the variables shown in [Table 133](#).

Table 133: Inbound Counters

Indicator Name	Inbound Counters
MIB	jnxFirewalls
Table	jnxFirewallCounterTable
Index	jnxFWFilter.jnxFWCounter
Variables	jnxFWCounterPacketCount jnxFWCounterByteCount
Description	Number of bytes being counted pertaining to the specified firewall filter counter
SNMP version	SNMPv2

This information can be collected by any SNMP management application that supports SNMPv2. Products from vendors such as Concord Communications, Inc., and InfoVista, Inc., provide support for the Juniper Networks Firewall MIB with their native Juniper Networks device drivers.

Monitoring Output Bytes per Queue

You can use the Juniper Networks enterprise ATM CoS MIB to monitor outbound traffic, per virtual circuit forwarding class, per interface. (See [Table 134](#).)

Table 134: Outbound Counters for ATM Interfaces

Indicator Name	Outbound Counters
MIB	JUNIPER-ATM-COS-MIB
Variable	jnxCosAtmVcQstatsOutBytes
Index	ifIndex.atmVclVpi.atmVclVci.jnxCosFcid

Table 134: Outbound Counters for ATM Interfaces (*continued*)

Indicator Name	Outbound Counters
Description	Number of bytes belonging to the specified forwarding class that were transmitted on the specified virtual circuit.
SNMP version	SNMPv2

Non-ATM interface counters are provided by the Juniper Networks enterprise-specific CoS MIB, which provides information shown in [Table 135](#).

Table 135: Outbound Counters for Non-ATM Interfaces

Indicator Name	Outbound Counters
MIB	JUNIPER-COS-MIB
Table	jnxCosIfqStatsTable
Index	jnxCosIfqIfIndex.jnxCosIfqFc
Variables	jnxCosIfqTxedBytes jnxCosIfqTxedPkts
Description	Number of transmitted bytes or packets per interface per forwarding class
SNMP version	SNMPv2

Dropped Traffic

You can calculate the amount of dropped traffic by subtracting the outbound traffic from the incoming traffic:

$$\text{Dropped} = \text{Inbound Counter} - \text{Outbound Counter}$$

You can also select counters from the CoS MIB, as shown in [Table 136](#).

Table 136: Dropped Traffic Counters

Indicator Name	Dropped Traffic
MIB	JUNIPER-COS-MIB
Table	jnxCosIfqStatsTable
Index	jnxCosIfqIfIndex.jnxCosIfqFc
Variables	jnxCosIfqTailDropPkts jnxCosIfqTotalRedDropPkts

Table 136: Dropped Traffic Counters (*continued*)

Indicator Name	Dropped Traffic
Description	The number of tail-dropped or RED-dropped packets per interface per forwarding class
SNMP version	SNMPv2

**Related
Documentation**

- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1643](#)
- [Understanding RMON for Monitoring Service Quality on page 1639](#)
- [Defining and Measuring Network Availability on page 1644](#)
- [Measuring Health on page 1650](#)

PART 19

Health Monitoring with SNMP

- [Configuring Health Monitoring on page 1667](#)

CHAPTER 73

Configuring Health Monitoring

- [Configuring Health Monitoring on Devices Running Junos OS on page 1667](#)
- [Example: Configuring Health Monitoring on page 1670](#)

Configuring Health Monitoring on Devices Running Junos OS

As the number of devices managed by a typical network management system (NMS) grows and the complexity of the devices themselves increases, it becomes increasingly impractical for the NMS to use polling to monitor the devices. A more scalable approach is to rely on network devices to notify the NMS when something requires attention.

On Juniper Networks routers, RMON alarms and events provide much of the infrastructure needed to reduce the polling overhead from the NMS. However, with this approach, you must set up the NMS to configure specific MIB objects into RMON alarms. This often requires device-specific expertise and customizing of the monitoring application. In addition, some MIB object instances that need monitoring are set only at initialization or change at runtime and cannot be configured in advance.

To address these issues, the health monitor extends the RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (for file system usage, CPU usage, and memory usage) and includes support for unknown or dynamic object instances (such as Junos OS processes).

Health monitoring is designed to minimize user configuration requirements. To configure health monitoring entries, include the **health-monitor** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
health-monitor {
  falling-threshold percentage;
  interval seconds;
  rising-threshold percentage;
}
```

You can use the **show snmp health-monitor** operational command to view information about health monitor alarms and logs.

This topic describes the minimum required configuration and discusses the following tasks for configuring the health monitor:

- [Monitored Objects on page 1668](#)
- [Minimum Health Monitoring Configuration on page 1669](#)
- [Configuring the Falling Threshold or Rising Threshold on page 1669](#)
- [Configuring the Interval on page 1669](#)
- [Log Entries and Traps on page 1670](#)

Monitored Objects

When you configure the health monitor, monitoring information for certain object instances is available, as shown in [Table 137](#).

Table 137: Monitored Object Instances

Object	Description
<code>jnxHrStoragePercentUsed.1</code>	Monitors the following file system on the router or switch: /dev/ad0s1a: This is the root file system mounted on <code>/</code> .
<code>jnxHrStoragePercentUsed.2</code>	Monitors the following file system on the router or switch: /dev/ad0s1e: This is the configuration file system mounted on <code>/config</code> .
<code>jnxOperatingCPU (RE0)</code> <code>jnxOperatingCPU (RE1)</code>	Monitors CPU usage for Routing Engines (RE0 and RE1). The index values assigned to Routing Engines depend on whether the Chassis MIB uses a zero-based or ones-based indexing scheme. Because the indexing scheme is configurable, the proper index is determined when the router or switch is initialized and when there is a configuration change. If the router or switch has only one Routing Engine, the alarm entry monitoring RE1 is removed after five failed attempts to obtain the CPU value.
<code>jnxOperatingBuffer (RE0)</code> <code>jnxOperatingBuffer (RE1)</code>	Monitors the amount of memory available on Routing Engines (RE0 and RE1). Because the indexing of this object is identical to that used for <code>jnxOperatingCPU</code> , index values are adjusted depending on the indexing scheme used in the Chassis MIB. As with <code>jnxOperatingCPU</code> , the alarm entry monitoring RE1 is removed if the router or switch has only one Routing Engine.
<code>sysAppElmtRunCPU</code>	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.
<code>sysAppElmtRunMemory</code>	Monitors the memory usage for each Junos OS process. Multiple instances of the same process are monitored and indexed separately.

Minimum Health Monitoring Configuration

To enable health monitoring on the router or switch, include the **health-monitor** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
health-monitor;
```

Configuring the Falling Threshold or Rising Threshold

The falling threshold is the lower threshold (expressed as a percentage of the maximum possible value) for the monitored variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising threshold. You must specify the falling threshold as a percentage of the maximum possible value. The default is **70** percent.

By default, the rising threshold is **80** percent of the maximum possible value for the monitored object instance. The rising threshold is the upper threshold for the monitored variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. You must specify the rising threshold as a percentage of the maximum possible value for the monitored variable.

To configure the falling threshold or rising threshold, include the **falling-threshold** or **rising-threshold** statement at the **[edit snmp health-monitor]** hierarchy level:

```
[edit snmp health-monitor]
falling-threshold percentage;
rising-threshold percentage;
```

percentage can be a value from 1 through 100.

The falling and rising thresholds apply to all object instances monitored by the health monitor.

Configuring the Interval

The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

To configure the interval, include the **interval** statement and specify the number of seconds at the **[edit snmp health-monitor]** hierarchy level:

```
[edit snmp health-monitor]
interval seconds;
```

seconds can be a value from 1 through 2147483647. The default is **300** seconds (5 minutes).

Log Entries and Traps

The system log entries generated for any health monitor events (thresholds crossed, errors, and so on) have a corresponding **HEALTHMONITOR** tag rather than a generic **SNMPD_RMON_EVENTLOG** tag. However, the health monitor sends generic RMON **risingThreshold** and **fallingThreshold** traps.

Related Documentation

- [Understanding RMON Alarms and Events Configuration on page 1625](#)
- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [Configuring an Event Entry and Its Attributes on page 1630](#)
- [Example: Configuring Health Monitoring on page 1670](#)
- *Understanding Device Management Functions in Junos OS*

Example: Configuring Health Monitoring

Configure the health monitor:

```
[edit snmp]
health-monitor {
  falling-threshold 85;
  interval 600;
  rising-threshold 75;
}
```

In this example, the sampling interval is every **600** seconds (10 minutes), the falling threshold is **85** percent of the maximum possible value for each object instance monitored, and the rising threshold is **75** percent of the maximum possible value for each object instance monitored.

Related Documentation

- [Configuring Health Monitoring on Devices Running Junos OS on page 1667](#)

PART 20

Gathering Statistics for Accounting Purposes Using Accounting Options, Source Class Usage and Destination Class Usage Options

- [Accounting Options, Source Class Usage and Destination Class Usage Options Overview on page 1673](#)
- [Configuring Accounting Options, Source Class Usage and Destination Class Usage Options on page 1677](#)

Accounting Options, Source Class Usage and Destination Class Usage Options Overview

- [Accounting Options Overview on page 1673](#)
- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)

Accounting Options Overview

An accounting profile represents common characteristics of collected accounting data, including the following:

- Collection interval
- File to contain accounting data
- Specific fields and counter names on which to collect statistics

You can configure multiple accounting profiles, as described in [Table 138](#).

Table 138: Types of Accounting Profiles

Type of Profile	Description
Interface profile	Collects the specified error and statistic information.
Filter profile	Collects the byte and packet counts for the counter names specified in the filter profile.
MIB profile	Collects selected MIB statistics and logs them to a specified file.
Routing Engine profile	Collects selected Routing Engine statistics and logs them to a specified file.
Class usage profile	Collects class usage statistics and logs them to a specified file.

Related Documentation

- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Accounting Options Configuration on page 1678](#)
- [Configuring Accounting-Data Log Files on page 1682](#)
- [Configuring the Interface Profile on page 1685](#)
- [Configuring the Filter Profile on page 1687](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1677](#)

Understanding Source Class Usage and Destination Class Usage Options

You can maintain packet counts based on the entry and exit points for traffic passing through your network. Entry and exit points are identified by source and destination prefixes grouped into disjoint sets defined as source classes and *destination classes*. You can define classes based on a variety of parameters, such as routing neighbors, autonomous systems, and route filters.

Source class usage (SCU) counts packets sent to customers by performing lookups on the IP source address and the IP destination address. SCU makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. You must enable SCU accounting on both the inbound and outbound physical interfaces.

Destination class usage (DCU) counts packets from customers by performing lookups of the IP destination address. DCU makes it possible to track traffic originating from the customer edge and destined for specific prefixes on the provider core router.

On T Series Core Routers and M320 Multiservice Edge Routers, the source class and destination classes are not carried across the platform fabric. The implications of this are as follows:

- On T Series and M320 routers, SCU and DCU accounting is performed before the packet enters the fabric.
- On T Series and M320 routers, DCU is performed before output filters are evaluated.
- On M Series platforms, DCU is performed after output filters are evaluated.
- If an output filter drops traffic on M Series devices, the dropped packets are excluded from DCU statistics.
- If an output filter drops traffic on T Series and M320 routers, the dropped packets are included in DCU statistics.



NOTE: SCU and DCU is supported on PTX series routers only when third-generation FPCs are installed on the router and *enhanced-mode* is configured on the chassis.

On MX Series platforms with MPC/MIC interfaces, SCU and DCU are performed after output filters are evaluated. Packets dropped by output filters are not included in SCU or DCU statistics.

On MX Series platforms with non-MPC/MIC interfaces, SCU and DCU are performed before output filters are evaluated. Packets dropped by output filters are included in SCU and DCU statistics.

On Enhanced Scaling FPCs (T640-FPC1-ES, T640-FPC2-ES, T640-FPC3-ES, T640-FPC4-1P-ES, and T1600-FPC4-ES), the source class accounting is performed at ingress. Starting with Junos OS Release 14.2, the SCU accounting is performed at ingress on a T4000 Type 5 FPC. The implications of this are as follows:

- SCU accounting is performed when packets traverse from T4000 Type 5 FPC (ingress FPC) to Enhanced Scaling FPCs (egress FPC).
- SCU accounting is performed when packets traverse from Enhanced Scaling FPCs (ingress FPC) to T4000 Type 5 FPC (egress FPC).



NOTE: When the interface statistics are cleared and then the routing engine is replaced, the SCU and DCU statistics will not match the statistics of the previous routing engine.

For more information about source class usage, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*, the *Junos OS Network Interfaces Library for Routing Devices*, and the *Junos OS, Release 15.1*.

**Related
Documentation**

- [Example: Grouping Source and Destination Prefixes into a Forwarding Class](#)
- [Configuring SCU or DCU on page 1691](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693](#)
- [Configuring Class Usage Profiles on page 1695](#)
- [Configuring the MIB Profile on page 1697](#)
- [Configuring the Routing Engine Profile on page 1699](#)

Configuring Accounting Options, Source Class Usage and Destination Class Usage Options

- Configuration Statements at the [edit accounting-options] Hierarchy Level on page 1677
- Accounting Options Configuration on page 1678
- Configuring Accounting-Data Log Files on page 1682
- Configuring the Interface Profile on page 1685
- Configuring the Filter Profile on page 1687
- Example: Configuring a Filter Profile on page 1689
- Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1690
- Configuring SCU or DCU on page 1691
- Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693
- Configuring Class Usage Profiles on page 1695
- Configuring the MIB Profile on page 1697
- Configuring the Routing Engine Profile on page 1699

Configuration Statements at the [edit accounting-options] Hierarchy Level

This topic shows all possible configuration statements at the **[edit accounting-options]** hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

```
[edit]
accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    destination-classes {
      destination-class-name;
    }
    source-classes {
      source-class-name;
    }
  }
}
```

```
}
file filename {
  archive-sites {
  }
  files number;
  nonpersistent;
  size bytes;
  start-time time;
  transfer-interval minutes;
}
filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}
}
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
mib-profile profile-name {
  file filename;
  interval seconds;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

- Related Documentation**
- [Accounting Options Overview on page 1673](#)
 - [Accounting Options Configuration on page 1678](#)

Accounting Options Configuration

This topic contains the following sections:

- [Accounting Options—Full Configuration on page 1679](#)
- [Minimum Accounting Options Configuration on page 1680](#)

Accounting Options—Full Configuration

To configure accounting options, include the following statements at the `[edit accounting-options]` hierarchy level:

```
accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    destination-classes {
      destination-class-name;
    }
    source-classes {
      source-class-name;
    }
    file filename {
      archive-sites {
        site-name;
      }
      files number;
      nonpersistent;
      size bytes;
      source-classes time
      transfer-interval minutes;
    }
    filter-profile profile-name {
      counters {
        counter-name;
      }
      file filename;
      interval minutes;
    }
  }
  interface-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
    interval seconds;
    object-names {
      mib-object-name;
    }
    operation operation-name;
  }
  routing-engine-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}
```

}

By default, accounting options are disabled.



NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Minimum Accounting Options Configuration

To enable accounting options on the router, you must perform at least the following tasks:

- Configure accounting options by including a **file** statement and one or more **source-class-usage**, **destination-class-profile**, **filter-profile**, **interface-profile**, **mib-profile**, or **routing-engine-profile** statements at the **[edit accounting-options]** hierarchy level:

```
[edit]
accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
      destination-classes {
        destination-class-name;
      }
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files number;
    size bytes;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
```



```

        mib-object-name;
    }
    operation operation-name;
}
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
}
}

```

- Apply the profiles to the chosen interfaces or filters.

Apply an interface profile to a physical or logical interface by including the **accounting-profile** statement at either the **[edit interfaces *interface-name*]** or the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

```

[edit interfaces]
interface-name {
    accounting-profile profile-name;
    unit logical-unit-number {
        accounting-profile profile-name;
    }
}

```



NOTE: You do not apply destination class profiles to interfaces. Although the interface needs to have the **destination-class-usage** statement configured, the destination class profile automatically finds all interfaces with the destination class configured.

Apply a filter profile to a firewall filter by including the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level:

```

[edit firewall]
filter filter-name {
    accounting-profile profile-name;
}

```

You do not need to apply the Routing Engine profile to an interface because the statistics are collected on the Routing Engine itself.

Related Documentation

- [Accounting Options Overview on page 1673](#)
- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Configuring Accounting-Data Log Files on page 1682](#)
- [Configuring the Interface Profile on page 1685](#)
- [Configuring the Filter Profile on page 1687](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1677](#)

Configuring Accounting-Data Log Files

An accounting profile specifies what statistics should be collected and written to a log file. To configure an accounting-data log file, include the **file** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
file filename {
  archive-sites {
    site-name;
  }
  files number;
  nonpersistent;
  size bytes;
  start-time time;
  transfer-interval minutes;
}
```

filename is the name of the file in which to write accounting data.

If the filename contains spaces, enclose it in quotation marks (" "). The filename cannot contain a forward slash (/). The file is created in the **/var/log** directory and can contain data from multiple profiles.

All accounting-data log files include header and trailer sections that start with a **#** in the first column. The header contains the file creation time, the hostname, and the columns that appear in the file. The trailer contains the time that the file was closed.

Whenever any configured value changes that affects the columns in a file, the file creates a new profile layout record that contains a new list of columns.

You must configure the file size; all other properties are optional.

- [Configuring the Storage Location of the File on page 1682](#)
- [Configuring the Maximum Size of the File on page 1683](#)
- [Configuring the Maximum Number of Files on page 1683](#)
- [Configuring the Start Time for File Transfer on page 1683](#)
- [Configuring the Transfer Interval of the File on page 1683](#)
- [Configuring Archive Sites on page 1684](#)

Configuring the Storage Location of the File

To configure the storage location of the files in the **mfs/var/log** directory (on DRAM) instead of the **cf/var/log** directory (on the compact flash drive), include the **nonpersistent** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
nonpersistent;
```

This feature is useful for minimizing read/write traffic on the router's compact flash drive.



NOTE: If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. Therefore, you should back up these files periodically.

Configuring the Maximum Size of the File

To configure the maximum size of the files, include the **size** statement at the **[edit accounting-options file *filename*]** hierarchy level:

```
[edit accounting-options file filename]  
size bytes;
```

The **size** statement is the maximum size of the log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). The minimum value for **bytes** is 256 KB. You must configure **bytes**; the remaining attributes are optional.

Configuring the Maximum Number of Files

To configure the maximum number of files, include the **files** statement at the **[edit accounting-options file *filename*]** hierarchy level:

```
[edit accounting-options file filename]  
files number;
```

When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for **number** is 3 and the default value is 10.

Configuring the Start Time for File Transfer

To configure the start time for transferring files, include the **start-time** statement at the **[edit accounting-options file *filename*]** hierarchy level:

```
[edit accounting-options file filename]  
start-time time;
```

The start-time statement specifies a start time for file transfer (**YYYY-MM-DD.hh:mm**). For example, 10:00 a.m. on January 30, 2007 is represented as **2007-01-30.10:00**.

Configuring the Transfer Interval of the File

To configure the transfer interval of the files, include the **transfer-interval** statement at the **[edit accounting-options file *filename*]** hierarchy level:

```
[edit accounting-options file filename]  
transfer-interval minutes;
```

The range for **transfer-interval** is 5 through 2880 minutes. The default is 30 minutes.



TIP:

Junos OS saves the existing log file and creates a new file at the configured transfer-intervals irrespective of:

- Whether the file has reached the maximum size or not
- Whether an archive site is configured or not

When you have a relatively smaller transfer-interval configured and if no archive site is configured, data can be lost as Junos OS overwrites the log files when the maximum number of log files is reached. To ensure that the log information is saved for a reasonably long time:

- Configure an archive site to archive the log files every time a new log file is created.
- Configure the maximum value (2880 minutes) for transfer-interval so that new files are created less frequently; that is, only when the file exceeds the maximum size limit or once in 2 days.

Configuring Archive Sites

After a file reaches its maximum size or the **transfer-interval** time is exceeded, the file is closed, renamed, and, if you configured an archive site, transferred to a remote host. To configure archive sites, include the **archive-sites** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
archive-sites {
  site-name;
}
```

site-name is any valid FTP URL. For more information about specifying valid FTP URLs, see the *Junos OS Administration Library for Routing Devices*. You can specify more than one URL, in any order. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, trying the next site in the list only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format **router-name_log-filename_timestamp**.

Related Documentation

- [Accounting Options Overview on page 1673](#)
- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Accounting Options Configuration on page 1678](#)
- [Configuring the Interface Profile on page 1685](#)
- [Configuring the Filter Profile on page 1687](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1677](#)

Configuring the Interface Profile

An interface profile specifies the information collected and written to a log file. You can configure a profile to collect error and statistic information for input and output packets on a particular physical or logical interface.

To configure an interface profile, include the **interface-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

By default, the Packet Forwarding Engine (PFE) periodically collects the statistics for all interfaces. To improve the performance, you can optionally disable the periodic refresh by including the **periodic-refresh disable** statement at the **[edit accounting-options]** hierarchy level.

Each accounting profile must have a unique **profile-name**. To apply a profile to a physical or logical interface, include the **accounting-profile** statement at either the **[edit interfaces interface-name]** or the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level. You can also apply an accounting profile at the **[edit firewall family family-type filter filter-name]** hierarchy level. For more information, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*.

To configure an interface profile, perform the tasks described in the following sections:

- [Configuring Fields on page 1685](#)
- [Configuring the File Information on page 1685](#)
- [Configuring the Interval on page 1686](#)
- [Example: Configuring the Interface Profile on page 1686](#)

Configuring Fields

An interface profile must specify what statistics are collected. To configure which statistics should be collected for an interface, include the **fields** statement at the **[edit accounting-options interface-profile profile-name]** hierarchy level:

```
[edit accounting-options interface-profile profile-name]
fields {
  field-name;
}
```

Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To configure which file to use, include the **file** statement at the **[edit accounting-options interface-profile *profile-name*]** hierarchy level:

```
[edit accounting-options interface-profile profile-name]  
file filename;
```

You must specify a **file** statement for the interface profile that has already been configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

Each interface with an accounting profile enabled has statistics collected once per interval time specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options interface-profile *profile-name*]** hierarchy level:

```
[edit accounting-options interface-profile profile-name]  
interval minutes;
```



NOTE: The minimum interval allowed is 1 minute. Configuring a low interval in an accounting profile for a large number of interfaces might cause serious performance degradation.

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

Example: Configuring the Interface Profile

Configure the interface profile:

```
[edit]  
accounting-options {  
  file if_stats {  
    size 40 files 5;  
  }  
  interface-profile if_profile1 {  
    file if_stats;  
    interval 30;  
    fields {  
      input-bytes;  
      output-bytes;  
      input-packets;  
      output-packets;  
      input-multicast;  
      output-multicast;  
    }  
  }  
  interface-profile if_profile2 {  
    file if_stats;  
    interval 30;  
    fields {  
      input-bytes;  
      output-bytes;  
      input-packets;  
      output-packets;  
      input-multicast;  
    }  
  }  
}
```

```

        output-multicast;
    }
}
interfaces {
    xe-1/0/0 {
        accounting-profile if_profile1;
        unit 0 {
            accounting-profile if_profile2;
            ...
        }
    }
}
}

```

The two interface profiles, **if-profile1** and **if-profile2**, write data to the same file, **if-stats**. The **if-stats** file might look like the following:

```

#FILE CREATED 976823478 2000-12-14-19:51:18
#hostname host
#profile-layout
if_profile2,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets,output-packets,input-multicast,output-multicast
#profile-layout
if_profile1,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets
if_profile2,976823538,xe-1/0/0.0,8,134696815,3681534,501088,40723,0,0
if_profile1,976823538,xe-1/0/0,7,134696815,3681534,501088
...
#FILE CLOSED 976824378 2000-12-14-20:06:18

```

Related Documentation

- [Accounting Options Overview on page 1673](#)
- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Accounting Options Configuration on page 1678](#)
- [Configuring Accounting-Data Log Files on page 1682](#)
- [Configuring the Filter Profile on page 1687](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1677](#)

Configuring the Filter Profile

A filter profile specifies error and statistics information collected and written to a file. A filter profile must specify counter names for which statistics are collected.

To configure a filter profile, include the **filter-profile** statement at the **[edit accounting-options]** hierarchy level:

```

[edit accounting-options]
filter-profile profile-name {
    counters {
        counter-name;
    }
    file filename;
    interval minutes;
}

```

```
}
```

To apply the filter profile, include the **accounting-profile** statement at the **[edit firewall filter *filter-name*]** hierarchy level.

To configure a filter profile, perform the tasks described in the following sections:

- [Configuring the Counters on page 1688](#)
- [Configuring the File Information on page 1688](#)
- [Configuring the Interval on page 1689](#)

Configuring the Counters

Statistics are collected for all counters specified in the filter profile. To configure the counters, include the **counters** statement at the **[edit accounting-options filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]  
counters {  
}
```

Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To configure which file to use, include the **file** statement at the **[edit accounting-options filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]  
file filename;
```

You must specify a filename for the filter profile that has already been configured at the **[edit accounting-options]** hierarchy level.



NOTE: The limit on the total number of characters per line in a log file equals 1023. If this limit is exceeded, the output written to the log file is incomplete. Ensure that you limit the number of counters or requested data so that this character limit is not exceeded.



NOTE: If the configured file size or transfer interval is exceeded, Junos OS closes the file and starts a new one. By default, the transfer interval value is 30 minutes. If the transfer interval is not configured, Junos OS closes the file and starts a new one when the file size exceeds its configured value or the default transfer interval value exceeds 30 minutes. To avoid transferring files every 30 minutes, specify a different value for the transfer interval.

Configuring the Interval

Each filter with an accounting profile enabled has statistics collected once per interval time specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options filter-profile *profile-name*]** hierarchy level:

```
[edit accounting-options filter-profile profile-name]  
interval;
```



NOTE: The minimum interval allowed is 1 minute. Configuring a low interval in an accounting profile for a large number of filters might cause serious performance degradation.

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

Related Documentation

- [Accounting Options Overview on page 1673](#)
- [Understanding Device Management Functions in Junos OS on page 1393](#)
- [Accounting Options Configuration on page 1678](#)
- [Configuring Accounting-Data Log Files on page 1682](#)

Example: Configuring a Filter Profile

Configure a filter profile:

```
[edit]  
accounting-options {  
  file fw_accounting {  
    size 500k files 4;  
  }  
  filter-profile fw_profile1 {  
    file fw_accounting;  
    interval 60;  
    counters {  
      counter1;  
      counter2;  
      counter3;  
    }  
  }  
}  
firewall {  
  filter myfilter {  
    accounting-profile fw_profile1;  
    ...  
    term accept-all {  
      then {  
        count counter1;  
        accept;  
      }  
    }  
  }  
}
```

```
}  
}
```

The filter profile, **fw-profile1**, writes data to the file **fw_accounting**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18  
#hostname host  
#profile-layout  
fw_profile1,epoch-timestamp,filter-name,counter-name,packet-count,byte-count  
fw_profile1,976826058,myfilter,counter1,163,10764  
...  
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

**Related
Documentation**

- [Configuring the Filter Profile on page 1687](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1690](#)

Example: Configuring Interface-Specific Firewall Counters and Filter Profiles

To collect and log count statistics collected by firewall filters on a per-interface basis, you must configure a filter profile and include the interface-specific statement at the **[edit firewall filter *filter-name*]** hierarchy level.

Configure the firewall filter accounting profile:

```
[edit accounting-options]  
file cust1_accounting {  
    size 500k;  
}  
filter-profile cust1_profile {  
    file cust1_accounting;  
    interval 1;  
    counters {  
        r1;  
    }  
}
```

Configure the interface-specific firewall counter:

```
[edit firewall]  
filter f3 {  
    accounting-profile cust1_profile;  
    interface-specific;  
    term f3-term {  
        then {  
            count r1;  
            accept;  
        }  
    }  
}
```

Apply the firewall filter to an interface:

```
[edit interfaces]  
xe-1/0/0 {  
    unit 0 {
```

```

family inet {
  filter {
    input f3;
    output f3;
  }
  address 20.20.20.30/24;
}
}

```

The following example shows the contents of the **cust1_accounting** file in the **/var/log** folder that might result from the preceding configuration:

```

#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
cust1_profile,995495572,xe-1/0/0.0,f3-xe-1/0/0.0-i,r1-xe-1/0/0.0-i,5953,1008257
cust1_profile,995495602,xe-1/0/0.0,f3-xe-1/0/0.0-o,r1-xe-1/0/0.0-o,5929,1006481
...

```

If the **interface-specific** statement is not included in the configuration, the following output might result:

```

#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
cust1_profile,995495572,xe-1/0/0.0,f3,r1,5953,1008257
cust1_profile,995495632,xe-1/0/0.0,f3,r1,5929,1006481

```

Related Documentation

- [Configuring the Filter Profile on page 1687](#)
- [Configuring the Interface Profile on page 1685](#)

Configuring SCU or DCU

To configure SCU or DCU, perform the following tasks described in this section:



NOTE: We recommend that you stop the network traffic on an interface before you modify the DCU or SCU configuration for that interface. Modifying the DCU or SCU configuration without stopping the traffic might corrupt the DCU or SCU statistics. Before you restart the traffic after modifying the configuration, enter the **clear interfaces statistics** command.

- [Creating Prefix Route Filters in a Policy Statement on page 1692](#)
- [Applying the Policy to the Forwarding Table on page 1692](#)
- [Enabling Accounting on Inbound and Outbound Interfaces on page 1692](#)

Creating Prefix Route Filters in a Policy Statement

To define prefix router filters:

```
[edit policy-options]
policy-statement scu-1 {
  term term1;
  from {
    route-filter 192.0.2.0/24 or longer;
  }
  then source-class gold;
}
```

Applying the Policy to the Forwarding Table

To apply the policy to the forwarding table:

```
[edit]
routing-options {
  forwarding-table {
    export scu-1;
  }
}
```

Enabling Accounting on Inbound and Outbound Interfaces

To enable accounting on inbound and outbound interfaces:

```
[edit]
interfaces {
  so-6/1/0 {
    unit 0 {
      family inet;
      accounting {
        destination-class-usage;
        source-class-usage {
          output;
        }
      }
    }
  }
}
[edit]
interfaces {
  xe-0/1/0 {
    unit 0 {
      family inet6 {
        accounting {
          source-class-usage {
            input;
          }
        }
      }
    }
  }
}
```

Optionally, you can include the input and output statements on a single interface as shown:

```
[edit]
interfaces {
  xe-0/1/2 {
    unit 0 {
      family inet6 {
        accounting {
          source-class-usage {
            input;
            output;
          }
        }
      }
    }
  }
}
```

For more information about configuring route filters and source classes in a routing policy, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices* and the *Junos OS Network Interfaces Library for Routing Devices*.

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693](#)
- [Configuring Class Usage Profiles on page 1695](#)
- [Configuring the MIB Profile on page 1697](#)
- [Configuring the Routing Engine Profile on page 1699](#)

Configuring SCU on a Virtual Loopback Tunnel Interface

To configure source class usage on the virtual loopback tunnel interface, perform the tasks described in the following sections:

- [Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC on page 1693](#)
- [Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface on page 1694](#)
- [Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface on page 1694](#)

Example: Configuring a Virtual Loopback Tunnel Interface on a Provider Edge Router Equipped with a Tunnel PIC

Define a virtual loop interface on a provider edge router with a Tunnel PIC:

```
[edit interfaces]
vt-0/3/0 {
  unit 0 {
    family inet {
      accounting {
```

```

        source-class-usage {
            input;
        }
    }
}

```

Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface

Map the VRF instance type to the virtual loopback tunnel interface:

```

[edit]
routing-instances {
  VPN-A {
    instance-type vrf;
    interface at-2/1/1.0;
    interface vt-0/3/0.0;
    route-distinguisher 10.255.14.225;
    vrf-import import-policy-name;
    vrf-export export-policy-name;
    protocols {
      bgp {
        group to-r4 {
          local-address 10.27.253.1;
          peer-as 400;
          neighbor 10.27.253.2;
        }
      }
    }
  }
}

```



NOTE: For SCU and DCU to work, do not include the `vrf-table-label` statement at the `[edit routing-instances instance-name]` hierarchy level.

Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface

Send traffic received from the virtual loopback tunnel interface out of the source class output interface:

```

[edit interfaces]
at-1/1/0 {
  unit 0 {
    family inet {
      accounting {
        source-class-usage {
          output;
        }
      }
    }
  }
}

```

For more information about configuring source class usage on the virtual loopback tunnel interface, see the *Junos OS Network Interfaces Library for Routing Devices*.

**Related
Documentation**

- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)
- [Configuring SCU or DCU on page 1691](#)
- [Configuring Class Usage Profiles on page 1695](#)
- [Configuring the MIB Profile on page 1697](#)
- [Configuring the Routing Engine Profile on page 1699](#)

Configuring Class Usage Profiles

To collect class usage statistics, perform the tasks described in these sections:

- [Configuring a Class Usage Profile on page 1695](#)
- [Configuring the File Information on page 1695](#)
- [Configuring the Interval on page 1696](#)
- [Creating a Class Usage Profile to Collect Source Class Usage Statistics on page 1696](#)
- [Creating a Class Usage Profile to Collect Destination Class Usage Statistics on page 1696](#)

Configuring a Class Usage Profile

You can configure the class usage profile to collect statistics for particular source and destination classes.

To configure the class usage profile to filter by source classes, include the **source-classes** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]  
source-classes {  
    source-class-name;  
}
```

To configure the class usage profile to filter by destination classes, include the **destination-classes** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]  
destination-classes {  
    destination-class-name;  
}
```

Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To specify which file to use, include the **file** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]  
file filename;
```

You must specify a filename for the source class usage profile that has already been configured at the **[edit accounting-options]** hierarchy level. You can also specify a filename for the destination class usage profile configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

Each interface with a class usage profile enabled has statistics collected once per interval specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options class-usage-profile *profile-name*]** hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]  
interval;
```

Creating a Class Usage Profile to Collect Source Class Usage Statistics

To create a class usage profile to collect source class usage statistics:

```
[edit]  
accounting-options {  
  class-usage-profile scu-profile1;  
  file usage-stats;  
  interval 15;  
  source-classes {  
    gold;  
    silver;  
    bronze;  
  }  
}
```

The class usage profile, **scu-profile1**, writes data to the file **usage_stats**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18  
#profile-layout, scu_profile, epoch-timestamp, interface-name, source-class,  
packet-count, byte-count  
scu_profile, 980313078, xe-1/0/0.0, gold, 82, 6888  
scu_profile, 980313078, xe-1/0/0.0, silver, 164, 13776  
scu_profile, 980313078, xe-1/0/0.0, bronze, 0, 0  
scu_profile, 980313678, xe-1/0/0.0, gold, 82, 6888  
scu_profile, 980313678, xe-1/0/0.0, silver, 246, 20664  
scu_profile, 980313678, xe-1/0/0.0, bronze, 0, 0
```

Creating a Class Usage Profile to Collect Destination Class Usage Statistics

To create a class usage profile to collect destination class usage statistics:

```
[edit]  
accounting-options {  
  class-usage-profile dcu-profile1;  
  file usage-stats  
  interval 15;  
  destination-classes {  
    gold;  
    silver;  
    bronze;
```



```
}
}
```

The class usage profile, **dcu-profile1**, writes data to the file **usage-stats**. The file might look like the following:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, dcu_profile,epoch-timestamp,interface-name,destination-class,
packet-count,byte-count
dcu_profile,980313078,xe-1/0/0.0,gold,82,6888
dcu_profile,980313078,xe-1/0/0.0,silver,164,13776
dcu_profile,980313078,xe-1/0/0.0,bronze,0,0
dcu_profile,980313678,xe-1/0/0.0,gold,82,6888
dcu_profile,980313678,xe-1/0/0.0,silver,246,20664
dcu_profile,980313678,xe-1/0/0.0,bronze,0,0
...
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)
- [Configuring SCU or DCU on page 1691](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693](#)
- [Configuring the Routing Engine Profile on page 1699](#)

Configuring the MIB Profile

The MIB profile collects MIB statistics and logs them to a file. The MIB profile specifies the SNMP operation and MIB object names for which statistics are collected.

To configure a MIB profile, include the **mib-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
mib-profile profile-name {
  file filename;
  interval minutes;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
```

To configure a MIB profile, perform the tasks described in the following sections:

- [Configuring the File Information on page 1697](#)
- [Configuring the Interval on page 1698](#)
- [Configuring the MIB Operation on page 1698](#)
- [Configuring MIB Object Names on page 1698](#)
- [Example: Configuring a MIB Profile on page 1698](#)

Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To configure which file to use, include the **file** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]  
  file filename;
```

You must specify a ***filename*** for the MIB profile that has already been configured at the **[edit accounting-options]** hierarchy level.

Configuring the Interval

A MIB profile has statistics collected once per interval time specified for the profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]  
  interval;
```

The range for the **interval** statement is 1 through 2880 minutes. The default is 30 minutes.

Configuring the MIB Operation

A MIB profile must specify the operation that is used to collect MIB statistics. To configure which operation is used to collect MIB statistics, include the **operation** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]  
  operation operation-name;
```

You can configure a **get**, **get-next**, or **walk** operation. The default operation is **walk**.

Configuring MIB Object Names

A MIB profile must specify the MIB objects for which statistics are to be collected. To configure the MIB objects for which statistics are collected, include the **objects-names** statement at the **[edit accounting-options mib-profile *profile-name*]** hierarchy level:

```
[edit accounting-options mib-profile profile-name]  
  object-names {  
    mib-object-name;  
  }
```

You can include multiple MIB object names in the configuration.



NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Example: Configuring a MIB Profile

Configure a MIB profile:

```
[edit accounting-options]  
  mib-profile mstatistics {  
    file stats;
```

```
interval 60;
operation walk;
objects-names {
  ipCidrRouteStatus;
}
}
```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)
- [Configuring SCU or DCU on page 1691](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693](#)
- [Configuring Class Usage Profiles on page 1695](#)
- [Configuring the Routing Engine Profile on page 1699](#)

Configuring the Routing Engine Profile

The Routing Engine profile collects Routing Engine statistics and logs them to a file. The Routing Engine profile specifies the fields for which statistics are collected.

To configure a Routing Engine profile, include the **routing-engine-profile** statement at the **[edit accounting-options]** hierarchy level:

```
[edit accounting-options]
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

To configure a Routing Engine profile, perform the tasks described in the following sections:

- [Configuring Fields on page 1699](#)
- [Configuring the File Information on page 1700](#)
- [Configuring the Interval on page 1700](#)
- [Example: Configuring a Routing Engine Profile on page 1700](#)

Configuring Fields

A Routing Engine profile must specify what statistics are collected. To configure which statistics should be collected for the Routing Engine, include the **fields** statement at the **[edit accounting-options routing-engine-profile *profile-name*]** hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]
fields {
  field-name;
}
```

Configuring the File Information

Each accounting profile logs its statistics to a file in the `/var/log` directory.

To configure which file to use, include the `file` statement at the `[edit accounting-options routing-engine-profile profile-name]` hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]  
file filename;
```

You must specify a *filename* for the Routing Engine profile that has already been configured at the `[edit accounting-options]` hierarchy level.

Configuring the Interval

A Routing Engine profile has statistics collected once per interval time specified for the profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the `interval` statement at the `[edit accounting-options routing-engine-profile profile-name]` hierarchy level:

```
[edit accounting-options routing-engine-profile profile-name]  
interval;
```

The range for `interval` is 1 through 2880 minutes. The default is 30 minutes.

Example: Configuring a Routing Engine Profile

Configure a Routing Engine profile:

```
[edit accounting-options]  
file my-file {  
  size 300k;  
}  
routing-engine-profile profile-1 {  
  file my-file;  
  fields {  
    host-name;  
    date;  
    time-of-day;  
    uptime;  
    cpu-load-1;  
    cpu-load-5;  
    cpu-load-15;  
  }  
}
```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1674](#)
- [Configuring SCU or DCU on page 1691](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1693](#)
- [Configuring Class Usage Profiles on page 1695](#)
- [Configuring the MIB Profile on page 1697](#)

PART 21

Configuring Monitoring Options

- [Configuring Interface Alarms on page 1703](#)
- [Using RPM to Measure Network Performance on page 1715](#)
- [Configuring IP Monitoring on page 1741](#)

CHAPTER 76

Configuring Interface Alarms

- [Alarm Overview on page 1703](#)
- [Example: Configuring Interface Alarms on page 1709](#)
- [Monitoring Active Alarms on a Device on page 1711](#)
- [Monitoring Alarms on page 1712](#)

Alarm Overview

Alarms alert you to conditions on a network interface, on the device chassis, or in the system software that might prevent the device from operating normally. You can set the conditions that trigger alarms on an interface. Chassis and system alarm conditions are preset.

An active alarm lights the **ALARM** LED on the front panel of the device. You can monitor active alarms from the J-Web user interface or the CLI. When an alarm condition triggers an alarm, the device lights the yellow (amber) **ALARM** LED on the front panel. When the condition is corrected, the light turns off.

This section contains the following topics:

- [Alarm Types on page 1703](#)
- [Alarm Severity on page 1704](#)
- [Alarm Conditions on page 1704](#)

Alarm Types

The device supports three types of alarms:

- Interface alarms indicate a problem in the state of the physical links on fixed or installed Physical Interface Modules (PIMs). To enable interface alarms, you must configure them.
- Chassis alarms indicate a failure on the device or one of its components. Chassis alarms are preset and cannot be modified.
- System alarms indicate a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web user interface or CLI.

Starting with Junos OS Release 15.1X49-D60, a new system alarm is introduced to indicate that the PICs (I/O card or SPC) have failed to come online during system start time.



NOTE: Run the following commands when the CLI prompt indicates that an alarm has been raised:

- `show system alarms`
- `show chassis alarms`
- `show chassis fpc pic-status`

For more information about the CLI commands, see [show system alarms](#), [show chassis alarms](#), and [show chassis fpc \(View\)](#).

Alarm Severity

Alarms have two severity levels:

- **Major (red)**—Indicates a critical situation on the device that has resulted from one of the following conditions. A red alarm condition requires immediate action.
 - One or more hardware components have failed.
 - One or more hardware components have exceeded temperature thresholds.
 - An alarm condition configured on an interface has triggered a critical warning.
- **Minor (yellow)**—Indicates a noncritical condition on the device that, if left unchecked, might cause an interruption in service or degradation in performance. A yellow alarm condition requires monitoring or maintenance.

A missing rescue configuration or software license generates a yellow system alarm.

Alarm Conditions

To enable alarms on a device interface, you must select an alarm condition and an alarm severity. In contrast, alarm conditions and severity are preconfigured for chassis alarms and system alarms.



NOTE: For information about chassis alarms for your device, see the [Hardware Guide](#) for your device.

This section contains the following topics:

- [Interface Alarm Conditions on page 1705](#)
- [System Alarm Conditions on page 1708](#)

Interface Alarm Conditions

Table 139 lists the interface conditions, sorted by interface type, that you can configure for an alarm. You can configure each alarm condition to trigger either a major (red) alarm or minor a (yellow) alarm. The corresponding configuration option is included.

For the services stateful firewall filters (NAT, IDP, and IPsec), which operate on an internal adaptive services module within a device, you can configure alarm conditions on the integrated services and services interfaces.

Table 139: Interface Alarm Conditions

Interface	Alarm Condition	Description	Configuration Option
DS1 (T1)	Alarm indication signal (AIS)	The normal T1 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	ylw
Ethernet	Link is down	The physical link is unavailable.	link-down
Integrated services	Hardware or software failure	On the adaptive services module, either the hardware associated with the module or the software that drives the module has failed.	failure

Table 139: Interface Alarm Conditions (*continued*)

Interface	Alarm Condition	Description	Configuration Option
Serial	Clear-to-send (CTS) signal absent	The remote endpoint of the serial link is not transmitting a CTS signal. The CTS signal must be present before data can be transmitted across a serial link.	cts-absent
	Data carrier detect (DCD) signal absent	The remote endpoint of the serial link is not transmitting a DCD signal. Because the DCD signal transmits the state of the device, no signal probably indicates that the remote endpoint of the serial link is unavailable.	dcd-absent
	Data set ready (DSR) signal absent	The remote endpoint of the serial link is not transmitting a DSR signal. The DSR signal indicates that the remote endpoint is ready to receive and transmit data across the serial link.	dsr-absent
	Loss of receive clock	The clock signal from the remote endpoint is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-rx-clock
	Loss of transmit clock	The local clock signal is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-tx-clock
Services	Services module hardware down	A hardware problem has occurred on the device's services module. This error typically means that one or more of the CPUs on the module has failed.	hw-down
	Services link down	The link between the device and its services module is unavailable.	linkdown
	Services module held in reset	The device's services module is stuck in reset mode. If the services module fails to start up five or more times in a row, the services module is held in reset mode. Startup fails when the amount of time from CPU release to CPU halt is less than 300 seconds.	pic-hold-reset
	Services module reset	The device's services module is resetting. The module resets after it crashes or is reset from the CLI, or when it takes longer than 60 seconds to start up.	pic-reset
	Services module software down	A software problem has occurred on the device's services module.	sw-down

Table 139: Interface Alarm Conditions (*continued*)

Interface	Alarm Condition	Description	Configuration Option
E3	Alarm indication signal (AIS)	The normal E3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Loss of signal (LOS)	No remote E3 signal is being received at the E3 interface.	los
	Out of frame (OOF)	An OOF condition has existed for 10 seconds. This alarm applies only to E3 interfaces configured in frame mode. The OOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds.	oof
	Remote defect indication	An AIS, LOS, or OOF condition exists. This alarm applies only to E3 interfaces configured in frame mode.	rdi

Table 139: Interface Alarm Conditions (*continued*)

Interface	Alarm Condition	Description	Configuration Option
T3 (DS3)	Alarm indication signal	The normal T3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Excessive number of zeros	The bit stream received from the upstream host has more consecutive zeros than are allowed in a T3 frame.	exz
	Far-end receive failure (FERF)	The remote endpoint of the connection has failed. A FERF differs from a yellow alarm, because the failure can be any failure, not just an OOF or LOS failure.	ferf
	Idle alarm	The Idle signal is being received from the remote endpoint.	idle
	Line code violation	Either the line encoding along the T3 link is corrupted or a mismatch between the encoding at the local and remote endpoints of a T3 connection occurred.	lcv
	Loss of frame (LOF)	An OOF or loss-of-signal LOS condition has existed for 10 seconds. The LOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds. A LOF failure is also called a red failure.	lof
	Loss of signal (LOS)	No remote T3 signal is being received at the T3 interface.	los
	Phase-locked loop out of lock	The clocking signals for the local and remote endpoints no longer operate in lock-step.	pll
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	ylw

System Alarm Conditions

Table 140 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 140: System Alarm Conditions and Corrective Actions

Alarm Type	Alarm Condition	Corrective Action
Configuration	The rescue configuration is not set.	Set the rescue configuration.

Table 140: System Alarm Conditions and Corrective Actions (*continued*)

Alarm Type	Alarm Condition	Corrective Action
License	<p>You have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed.</p> <p>NOTE: This alarm indicates that you are in violation of the software license agreement. You must install a valid license key to be in compliance with all agreements.</p>	Install a valid license key.

- Related Documentation**
- [Example: Configuring Interface Alarms on page 1709](#)
 - [Monitoring Active Alarms on a Device on page 1711](#)
 - [Monitoring Alarms on page 1712](#)
 - [System Log Messages](#)

Example: Configuring Interface Alarms

This example shows how to configure interface alarms.

- [Requirements on page 1709](#)
- [Overview on page 1709](#)
- [Configuration on page 1710](#)
- [Verification on page 1711](#)

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.
- Select the network interface on which to apply an alarm and the condition you want to trigger the alarm. See [“Alarm Overview” on page 1703](#).

Overview

In this example, you enable interface alarms by explicitly setting alarm conditions. You configure the system to generate a red interface alarm when a yellow alarm is detected on a DS1 link. You configure the system to generate a red interface alarm when a link-down failure is detected on an Ethernet link.

For a serial link, you set cts-absent and dcd-absent to yellow to signify either the CST or the DCD signal is not detected. You set loss-of-rx-clock and loss-of-tx-clock to red alarm to signify either the receiver clock signal or the transmission clock signal is not detected.

For a T3 link, you set the interface alarm to red when the remote endpoint is experiencing a failure. You set exz to yellow alarm when the upstream bit has more consecutive zeros than are permitted in a T3 interface. You then set a red alarm when there is loss-of-signal on the interface.

Finally, you configure the system to display active system alarms whenever a user with the login class admin logs in to the device.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set chassis alarm ds1 ylw red
set chassis alarm ethernet link-down red
set chassis alarm serial cts-absent yellow dcd-absent yellow
set chassis alarm serial loss-of-rx-clock red loss-of-tx-clock red
set chassis alarm t3 ylw red exz yellow los red
set system login class admin login-alarms
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure interface alarms:

1. Configure an alarm.

```
[edit]
user@host# edit chassis alarm
```

2. Specify the interface alarms on a DS1 and an Ethernet link.

```
[edit chassis alarm]
user@host# set ds1 ylw red
user@host# set ethernet link-down red
```

3. Specify the interface alarms on a serial link.

```
[edit chassis alarm]
user@host# set serial cts-absent yellow
user@host# set serial dcd-absent yellow
user@host# set serial loss-of-rx-clock red
user@host# set serial loss-of-tx-clock red
```

4. Specify the interface alarms on a T3 link.

```
[edit chassis alarm]
user@host# set t3 ylw red
user@host# set t3 exz yellow
user@host# set t3 los red
```

5. Configure the system to display active system alarms.

```
[edit]
user@host# edit system login
```

```
user@host# set class admin login-alarms
```

Results From configuration mode, confirm your configuration by entering the **show chassis alarms** and **show system login** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis alarms
t3 {
  exz yellow;
  los red;
  ylw red;
}
ds1 {
  ylw red;
}
ethernet {
  link-down red;
}
serial {
  loss-of-rx-clock red;
  loss-of-tx-clock red;
  dcd-absent yellow;
  cts-absent yellow;
}
[edit]
user@host# show system login
show system login
show system login
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Verifying the Alarm Configurations

Purpose Confirm that the configuration is working properly.

Verify that the alarms are configured.

Action From configuration mode, enter the **show chassis alarms** command. Verify that the output shows the intended configuration of the alarms.

Related Documentation

- [Alarm Overview on page 1703](#)
- [Monitoring Active Alarms on a Device on page 1711](#)
- [Monitoring Alarms on page 1712](#)

Monitoring Active Alarms on a Device

Purpose Use to monitor and filter alarms on a Juniper Networks device.

Action Select **Monitor>Events and Alarms>View Alarms** in the J-Web user interface. The J-Web View Alarms page displays the following information about preset system and chassis alarms:

- Type—Type of alarm: System, Chassis, or All.
- Severity—Severity class of the alarm: Minor or Major.
- Description—Description of the alarm.
- Time—Time that the alarm was registered.

To filter which alarms appear, use the following options:

- Alarm Type—Specifies which type of alarm to monitor: System, Chassis, or All. System alarms include FRU detection alarms (power supplies removed, for instance). Chassis alarms indicate environmental alarms such as temperature.
- Severity—Specifies the alarm severity that you want to monitor: Major, Minor, or All. A major (red) alarm condition requires immediate action. A minor (yellow) condition requires monitoring and maintenance.
- Description—Specifies the alarms you want to monitor. Enter a brief synopsis of the alarms that you want to monitor.
- Date From—Specifies the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.
- To—Specifies the end of the date range that you want to monitor. Set the date using the calendar pick tool.
- Go—Executes the options that you specified.
- Reset—Clears the options that you specified.

Alternatively, you can enter the following **show** commands in the CLI editor:

- **show chassis alarms**
- **show system alarms**

- Related Documentation**
- [Alarm Overview on page 1703](#)
 - [Example: Configuring Interface Alarms on page 1709](#)
 - [Monitoring Alarms on page 1712](#)

Monitoring Alarms

Purpose Use the monitoring functionality to view the alarms page.

Action To monitor alarms select **Monitor>Events and Alarms>View Alarms** in the J-Web user interface.

Meaning [Table 141](#) summarizes key output fields in the alarms page.

Table 141: Alarms Monitoring Page

Field	Value	Additional Information
Alarm Filter		
Alarm Type	Specifies the type of alarm to monitor: <ul style="list-style-type: none"> • System— System alarms include FRU detection alarms (power supplies removed, for instance). • Chassis— Chassis alarms indicate environmental alarms such as temperature. • All— Indicates to display all the types of alarms. 	—
Severity	Specifies the alarm severity that you want to monitor <ul style="list-style-type: none"> • Major— A major (red) alarm condition requires immediate action. • Minor— A minor (yellow) condition requires monitoring and maintenance. • All— Indicates to display all the severities. 	—
Description	Enter a brief synopsis of the alarms you want to monitor.	—
Date From	Specifies the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.	—
To	Specifies the end of the date range that you want to monitor. Set the date using the calendar pick tool.	—
Go	Executes the options that you specified.	—
Reset	Clears the options that you specified.	—
Alarm Details	Displays the following information about each alarm: <ul style="list-style-type: none"> • Type— Type of alarm: System, Chassis, or All. • Severity— Severity class of the alarm: Minor or Major. • Description— Description of the alarm. • Time— Time that the alarm was registered. 	—

- Related Documentation**
- [Monitoring Active Alarms on a Device on page 1711](#)
 - [Monitoring Events on page 1845](#)

- [Monitoring Security Events by Policy on page 1827](#)

CHAPTER 77

Using RPM to Measure Network Performance

- [RPM Overview on page 1715](#)
- [IPv6 RPM Probes on page 1719](#)
- [Guidelines for Configuring RPM Probes for IPv6 on page 1719](#)
- [RPM Support for VPN Routing and Forwarding on page 1721](#)
- [Example: Configuring Basic RPM Probes on page 1721](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1725](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1728](#)
- [Directing RPM Probes to Select BGP Devices on page 1730](#)
- [Configuring IPv6 RPM Probes on page 1731](#)
- [Tuning RPM Probes on page 1732](#)
- [RPM Configuration Options on page 1732](#)
- [Monitoring RPM Probes on page 1736](#)

RPM Overview

The real-time performance monitoring (RPM) feature allows network operators and their customers to accurately measure the performance between two network endpoints. With the RPM tool, you configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter.

RPM allows you to perform service-level monitoring. When RPM is configured on a device, the device calculates network performance based on packet response time, jitter, and packet loss. These values are gathered by Hypertext Transfer Protocol (HTTP) GET requests, Internet Control Message Protocol (ICMP) requests, and TCP and UDP requests, depending on the configuration.

This section contains the following topics:

- [RPM Probes on page 1716](#)
- [RPM Tests on page 1716](#)
- [Probe and Test Intervals on page 1716](#)

- [Jitter Measurement with Hardware Timestamping on page 1717](#)
- [RPM Statistics on page 1717](#)
- [RPM Thresholds and Traps on page 1718](#)
- [RPM for BGP Monitoring on page 1719](#)

RPM Probes

You gather RPM statistics by sending out probes to a specified probe target, identified by an IP address or URL. When the target receives the probe, it generates responses, which are received by the device. By analyzing the transit times to and from the remote server, the device can determine network performance statistics.

The device sends out the following probe types:

- HTTP GET request at a target URL
- HTTP GET request for metadata at a target URL
- ICMP echo request to a target address (the default)
- ICMP timestamp request to a target address
- UDP ping packets to a target device
- UDP timestamp requests to a target address
- TCP ping packets to a target device

UDP and TCP probe types require that the remote server be configured as an RPM receiver so that it generates responses to the probes.

The RPM probe results are also available in the form of MIB objects through the SNMP protocol.

RPM Tests

Each probed target is monitored over the course of a test. A test represents a collection of probes, sent out at regular intervals, as defined in the configuration. Statistics are then returned for each test. Because a test is a collection of probes that have been monitored over some amount of time, test statistics such as standard deviation and jitter can be calculated and included with the average probe statistics.

Probe and Test Intervals

Within a test, RPM probes are sent at regular intervals, configured in seconds. When the total number of probes has been sent and the corresponding responses received, the test is complete. You can manually set the probe interval for each test to control how the RPM test is conducted.

After all the probes for a particular test have been sent, the test begins again. The time between tests is the test interval. You can manually set the test interval to tune RPM performance.



NOTE: On SRX340 Low Memory devices and SRX340 High Memory devices, the RPM server operation does not work when the probe is configured with the option destination-interface.

Jitter Measurement with Hardware Timestamping

Jitter is the difference in relative transit time between two consecutive probes.

You can timestamp the following RPM probes to improve the measurement of latency or jitter:

- ICMP ping
- ICMP ping timestamp
- UDP ping
- UDP ping timestamp



NOTE: The device supports hardware timestamping of UDP ping and UDP ping timestamp RPM probes only if the destination port is UDP-ECHO (port 7).

Timestamping takes place during the forwarding process of the device originating the probe (the RPM client), but not on the remote device that is the target of the probe (the RPM server).

The supported encapsulations on a device for timestamping are Ethernet including VLAN, synchronous PPP, and Frame Relay. The only logical interface supported is an *lt* services interface.

RPM probe generation with hardware timestamp can be retrieved through the SNMP protocol.

RPM Statistics

At the end of each test, the device collects the statistics for packet round-trip time, packet inbound and outbound times (for ICMP timestamp probes only), and probe loss as shown in [Table 142](#).

Table 142: RPM Statistics

RPM Statistics	Description
Round-Trip Times	
Minimum round-trip time	Shortest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test
Maximum round-trip time	Longest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test

Table 142: RPM Statistics (*continued*)

RPM Statistics	Description
Average round-trip time	Average round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test
Standard deviation round-trip time	Standard deviation of the round-trip times from the Juniper Networks device to the remote server, as measured over the course of the test
Jitter	Difference between the maximum and minimum round-trip times, as measured over the course of the test
Inbound and Outbound Times (ICMP Timestamp Probes Only)	
Minimum egress time	Shortest one-way time from the Juniper Networks device to the remote server, as measured over the course of the test
Maximum ingress time	Shortest one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Average egress time	Average one-way time from the Juniper Networks device to the remote server, as measured over the course of the test
Average ingress time	Average one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Standard deviation egress time	Standard deviation of the one-way times from the Juniper Networks device to the remote server, as measured over the course of the test
Standard deviation ingress time	Standard deviation of the one-way times from the remote server to the Juniper Networks device, as measured over the course of the test
Egress jitter	Difference between the maximum and minimum outbound times, as measured over the course of the test
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
Probe Counts	
Probes sent	Total number of probes sent over the course of the test
Probe responses received	Total number of probe responses received over the course of the test
Loss percentage	Percentage of probes sent for which a response was not received

RPM Thresholds and Traps

You can configure RPM threshold values for the round-trip times, ingress (inbound) times, and egress (outbound) times that are measured for each probe, as well as for the standard deviation and jitter values that are measured for each test. Additionally, you can configure threshold values for the number of successive lost probes within a test and the total number of lost probes within a test.

If the result of a probe or test exceeds any threshold, the device generates a system log message and sends any Simple Network Management Protocol (SNMP) notifications (traps) that you have configured.

RPM for BGP Monitoring

When managing peering networks that are connected using Border Gateway Protocol (BGP), you might need to find out if a path exists between the Juniper Networks device and its configured BGP neighbors. You can ping each BGP neighbor manually to determine the connection status, but this method is not practical when the device has a large number of BGP neighbors configured.

In the device, you can configure RPM probes to monitor the BGP neighbors and determine if they are active.

Related Documentation

- [RPM Configuration Options on page 1732](#)
- [RPM Support for VPN Routing and Forwarding on page 1721](#)
- [Example: Configuring Basic RPM Probes on page 1721](#)
- [Monitoring RPM Probes on page 1736](#)
- [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1957](#)

IPv6 RPM Probes

Starting with Junos OS Release 15.1X49-D10, Route Engine-based RPM can send and receive IPv6 probe packets to monitor performance on IPv6 networks.

A probe request is a standard IPv6 packet with corresponding TCP, UDP, and ICMPv6 headers. A probe response is also a standard IPv6 packet with corresponding TCP, UDP, and ICMPv6 headers. No RPM header is appended to the standard packet for RE-based RPM. An IPv6-based RPM test occurs between an IPv6 RPM client and IPv6 RPM server.



NOTE: You can have both IPv4 tests and IPv6 tests in the same probe.

Related Documentation

- [Guidelines for Configuring RPM Probes for IPv6 on page 1719](#)
- [Configuring IPv6 RPM Probes on page 1731](#)

Guidelines for Configuring RPM Probes for IPv6

Keep the following guidelines in mind when you configure IPv6 addresses for RPM destinations or servers:

- IPv6 RPM uses ICMPv6 probe requests. You cannot configure ICMP or ICMP timestamp probe types.
- Only Routing Engine-based RPM is supported for IPv6 targets including VRF support, specification of the size of the data portion of ICMPv6 probes, data pattern, and traffic class.
- You can configure probes with a combination of IPv4 and IPv6 tests. However, an individual test must be either IPv4 or IPv6.
- Routing Engine-based RPM does not support hardware-based, or one-way hardware-based timestamping.
- We recommend that you include the **probe-limit** statement at the **[edit services rpm]** hierarchy level to set the limit on concurrent probes to 10. Higher concurrent probes can result in higher spikes.
- SNMP set operation is permitted only on ICMP probes and it is not supported for other probe types.
- The following table describes the IPv6 special address prefixes that you cannot configure in a probe.

IPv6 Address Type	IPv6 Address Prefix
Node-Scoped Unicast	::1/128 is the loopback address ::/128 is the unspecified address
IPv4-Mapped Addresses	::FFFF:0:0/96
IPv4-Compatible Addresses	:<ipv4-address>/96
Link-Scoped Unicast	fe80::/10
Unique-Local	fc00::/7
Documentation Prefix	2001:db8::/32
6to4	2002::/16
6bone	5f00::/8
ORCHID	2001:10::/28
Teredo	2001::/32
Default Route	::/0
Multicast	ff00::/8

- In Routing Engine-based RPM, route-trip time (RTT) spikes might occur because of queuing delays, even with a single test.
- Since RPM might open TCP and UDP ports to communicate between the RPM server and RPM client, we recommend that you use firewalls and distributed denial-of-service (DDoS) attack filters to protect against security threats.

**Related
Documentation**

- [Configuring IPv6 RPM Probes on page 1731](#)

RPM Support for VPN Routing and Forwarding

Real-time performance monitoring (RPM) is supported on all Juniper Network devices.

VRF in a Layer 3 VPN implementation allows multiple instances of a routing table to coexist within the same device at the same time. Because the routing instances are independent, the same or overlapping IPv4 or IPv6 addresses can be used without conflicting each other.

RPM ICMP and UDP probe with VPN routing and forwarding (VRF) has been improved. In previous releases, the RPM probes specified to a VRF table were not handled by the real-time forwarding process (FWDD-RT). In Junos OS Release 10.0, RPM probes specified to a VRF table are handled by the FWDD-RT, thereby providing more accurate results.

This feature supports RPM ICMP and UDP probes configured with routing instances of type VRF.

**Related
Documentation**

- [RPM Overview on page 1715](#)
- [RPM Configuration Options on page 1732](#)
- [Monitoring RPM Probes on page 1736](#)

Example: Configuring Basic RPM Probes

This example shows how to configure basic RPM probes to measure performance between two network endpoints.

- [Requirements on page 1721](#)
- [Overview on page 1722](#)
- [Configuration on page 1722](#)
- [Verification on page 1724](#)

Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.

Overview

In this example, you configure basic probes for two RPM owners, customerA and customerB. You configure the RPM test as icmp-test for customerA with a test interval of 15 seconds and specify a probe type as icmp-ping-timestamp, a probe timestamp, and a target address as 192.178.16.5. You then configure the RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.

Then you configure the RPM test as http-test for customerB with a test interval of 30 seconds and specify a probe type as http-get and a target URL as http://customerB.net. Finally, you configure RPM thresholds and corresponding SNMP traps as probe-failure and test-failure to catch three or more successive lost probes and total lost probes of 10.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services rpm probe customerA test icmp-test probe-interval 15
set services rpm probe customerA test icmp-test probe-type icmp-ping-timestamp
set services rpm probe customerA test icmp-test hardware-timestamp
set services rpm probe customerA test icmp-test target address 192.178.16.5
set services rpm probe customerA test icmp-test thresholds ingress-time 3000
set services rpm probe customerA test icmp-test traps ingress-time-exceeded
set services rpm probe customerB test http-test probe-interval 30
set services rpm probe customerB test http-test probe-type http-get
set services rpm probe customerB test http-test target url http://customerB.net
set services rpm probe customerB test http-test thresholds successive-loss 3
set services rpm probe customerB test http-test thresholds total-loss 10
set services rpm probe customerB test http-test traps probe-failure
set services rpm probe customerB test http-test traps test-failure
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure basic RPM probes:

1. Configure the RPM.

```
[edit]
user@host# edit services rpm
```
2. Configure the RPM owners.

```
[edit services rpm]
user@host# set probe customerA
user@host# set probe customerB
```
3. Configure the RPM test for customerA.

- ```
[edit services rpm]
user@host# edit probe customerA
user@host# set test icmp-test probe-interval 15
user@host# set test icmp-test probe-type icmp-ping-timestamp
```
4. Specify a probe timestamp and a target address.
 

```
[edit services rpm probe customerA]
user@host# set test icmp-test hardware-timestamp
user@host# set test icmp-test target address 192.178.16.5
```
  5. Configure RPM thresholds and corresponding SNMP traps.
 

```
[edit services rpm probe customerA]
user@host# set test icmp-test thresholds ingress-time 3000
user@host# set test icmp-test traps ingress-time-exceeded
```
  6. Configure the RPM test for customerB.
 

```
[edit]
user@host# edit services rpm probe customerB
user@host# set test http-test probe-interval 30
```
  7. Specify a probe type and a target URL.
 

```
[edit services rpm probe customerB]
user@host# set test http-test probe-type http-get
user@host# set test http-test target url http://customerB.net
```
  8. Configure RPM thresholds and corresponding SNMP traps.
 

```
[edit services rpm probe customerB]
user@host# set test http-test thresholds successive-loss 3
user@host# set test http-test thresholds total-loss 10
user@host# set test http-test traps probe-failure
user@host# set test http-test traps test-failure
```

**Results** From configuration mode, confirm your configuration by entering the **show services rpm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services rpm
probe customerA {
 test icmp-test {
 probe-type icmp-ping-timestamp;
 target address 192.0.2.2;
 probe-interval 15;
 thresholds {
 ingress-time 3000;
 }
 traps ingress-time-exceeded;
 hardware-timestamp;
 }
}
probe customerB {
 test http-test {
 probe-type http-get
 target url http://customerB.net;
```

```
 probe-interval 30;
 thresholds {
 successive-loss 3;
 total-loss 10;
 }
 traps [probe-failure test-failure];
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Verifying RPM Services on page 1724](#)
- [Verifying RPM Statistics on page 1724](#)

---

### Verifying RPM Services

**Purpose** Verify that the RPM configuration is within the expected values.

**Action** From configuration mode, enter the **show services rpm** command. The output shows the values that are configured for RPM on the device.

---

### Verifying RPM Statistics

**Purpose** Verify that the RPM probes are functioning and that the RPM statistics are within expected values.

**Action** From configuration mode, enter the **show services rpm probe-results** command.

```
user@host> show services rpm probe-results
```

```
Owner: customerD, Test: icmp-test
Probe type: icmp-ping-timestamp
Minimum Rtt: 312 usec, Maximum Rtt: 385 usec, Average Rtt: 331 usec,
Jitter Rtt: 73 usec, Stddev Rtt: 27 usec
Minimum egress time: 0 usec, Maximum egress time: 0 usec,
Average egress time: 0 usec, Jitter egress time: 0 usec,
Stddev egress time: 0 usec
Minimum ingress time: 0 usec, Maximum ingress time: 0 usec,
Average ingress time: 0 usec, Jitter ingress time: 0 usec,
Stddev ingress time: 0 usec
Probes sent: 5, Probes received: 5, Loss percentage: 0
```

```
Owner: customerE, Test: http-test
Target address: 192.176.17.4, Target URL: http://customerB.net,
Probe type: http-get
Minimum Rtt: 1093 usec, Maximum Rtt: 1372 usec, Average Rtt: 1231 usec,
Jitter Rtt: 279 usec, Stddev Rtt: 114 usec
Probes sent: 3, Probes received: 3, Loss percentage: 0
```

```
Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
Routing Instance Name: LR1/RI1
```

```

Probe results:
 Response received, Fri Oct 28 05:20:23 2005
 Rtt: 662 usec
Results over current test:
 Probes sent: 5, Probes received: 5, Loss percentage: 0
 Measurement: Round trip time
 Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
 Jitter: 133 usec, Stddev: 53 usec
Results over all tests:
 Probes sent: 5, Probes received: 5, Loss percentage: 0
 Measurement: Round trip time
 Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
 Jitter: 133 usec, Stddev: 53 usec

```

- Related Documentation**
- [RPM Overview on page 1715](#)
  - [RPM Configuration Options on page 1732](#)
  - [Tuning RPM Probes on page 1732](#)

## Example: Configuring RPM Using TCP and UDP Probes

This example shows how to configure RPM using TCP and UDP probes.

- [Requirements on page 1725](#)
- [Overview on page 1725](#)
- [Configuration on page 1726](#)
- [Verification on page 1727](#)

### Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.
- Configure the probe owner, the test, and the specific parameters of the RPM probe. See [“Example: Configuring Basic RPM Probes” on page 1721](#).

### Overview

In this example, you configure both the host (device A) and the remote device (device B) to act as TCP and UDP servers. You configure a probe for customerC, which uses TCP packets. Device B is configured as an RPM server for both TCP and UDP packets, using an *lt* services interface as the destination interface, and ports 50000 and 50037, respectively.



**CAUTION:** Use probe classification with caution, because improper configuration can cause packets to be dropped.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
{device A}
set services rpm probe customerC test tcp-test probe-interval 5
set services rpm probe customerC test tcp-test probe-type tcp-ping
set services rpm probe customerC test tcp-test target address 192.162.45.6
set services rpm probe customerC test tcp-test destination-interface lt-0/0/0
set services rpm probe customerC test tcp-test destination-port 50000

{device B}
set services rpm probe-server tcp port 50000
set services rpm probe-server udp port 50037
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure RPM using TCP and UDP probes:

1. Configure the RPM owner on device A.

```
{device A}
[edit]
user@host# edit services rpm
user@host# set probe customerC
```

2. Configure the RPM test.

```
{device A}
[edit services rpm]
user@host# edit services rpm probe customerC
user@host# set test tcp-test probe-interval 5
```

3. Set the probe type.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test probe-type tcp-ping
```

4. Specify the target address.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test target address 192.162.45.6
```

5. Configure the destination interface.

```
{device A}
[edit services rpm probe customerC]
user@host# set test tcp-test destination-interface lt-0/0/0
```

6. Configure port 50000 as the TCP port to which the RPM probes are sent.

```
{device A}
```

```
[edit services rpm probe customerC]
user@host# set test tcp-test destination-port 50000
```

7. Configure device B to act as a TCP server using port 50000.

```
{device B}
[edit]
user@host# edit services rpm
user@host# set probe-server tcp port 50000
```

8. Configure device B to act as a UDP server using port 50037.

```
{device B}
[edit services rpm]
user@host# set probe-server udp port 50037
```

**Results** From configuration mode, confirm your configuration by entering the **show services rpm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services rpm
probe customerC {
 test tcp-test {
 probe-type tcp-ping;
 target address 192.162.45.6;
 probe-interval 5;
 destination-port 50000;
 destination-interface lt-0/0/0.0;
 }
}
probe-server {
 tcp {
 port 50000;
 }
 udp {
 port 50037;
 }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying RPM Probe Servers

**Purpose** Confirm that the configuration is working properly.

Verify that the device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

**Action** From configuration mode, enter the **show services rpm active-servers** command. The output shows a list of the protocols and corresponding ports for which the device is configured as an RPM server.

```
user@host> show services rpm active-servers
```

```
Protocol: TCP, Port: 50000
```

```
Protocol: UDP, Port: 50037
```

#### Related Documentation

- [RPM Overview on page 1715](#)
- [RPM Configuration Options on page 1732](#)
- [Example: Configuring Basic RPM Probes on page 1721](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1728](#)
- [Tuning RPM Probes on page 1732](#)

---

## Example: Configuring RPM Probes for BGP Monitoring

This example shows how to configure RPM probes to monitor BGP neighbors.

- [Requirements on page 1728](#)
- [Overview on page 1728](#)
- [Configuration on page 1729](#)
- [Verification on page 1730](#)

### Requirements

Before you begin:

- Configure the BGP parameters under RPM configuration to send RPM probes to BGP neighbors. See [“Example: Configuring Basic RPM Probes” on page 1721](#).
- Use TCP or UDP probes by configure both the probe server (Juniper Networks device) and the probe receiver (the remote device) to transmit and receive RPM probes on the same TCP or UDP port. See [“Example: Configuring RPM Using TCP and UDP Probes” on page 1725](#).

### Overview

In this example, you specify a hexadecimal value that you want to use for the data portion of the RPM probe as ABCD123. ( It ranges from 1 through 2048 characters.) You specify the data size of the RPM probe as 1024 bytes. ( The value ranges from 0 through 65,507.)

Then you configure destination port 50000 as the TCP port to which the RPM probes are sent. You specify the number of probe results to be saved in the probe history as 25. (It ranges from 0 through 255, and the default is 50.) You set the probe count to 5 and probe interval as 1. (The probe count ranges from 1 through 15, and the default is 1; and the probe interval ranges from 1 through 255, and the default is 3.) You then specify tcp-ping as the type of probe to be sent as part of the test.

Finally, you set the test interval as 60. The value ranges from 0 through 86,400 seconds for the interval between tests.



## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services rpm bgp data-fill ABCD123 data-size 1024
set services rpm bgp destination-port 50000 history-size 25
set services rpm bgp probe-count 5 probe-interval 1
set services rpm bgp probe-type tcp-ping test-interval 60
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure RPM probes to monitor BGP neighbors:

1. Configure the RPM and BGP.  

```
[edit]
user@host# edit services rpm bgp
```
2. Specify a hexadecimal value.  

```
[edit services rpm bgp]
user@host# set data-fill ABCD123
```
3. Specify the data size of the RPM probe.  

```
[edit services rpm bgp]
user@host# set data-size 1024
```
4. Configure the destination port.  

```
[edit services rpm bgp]
user@host# set destination-port 50000
```
5. Specify the number of probes.  

```
[edit services rpm bgp]
user@host# set history-size 25
```
6. Set the probe count and probe interval.  

```
[edit services rpm bgp]
user@host# set probe-count 5 probe-interval 1
```
7. Specify the type of probe.  

```
[edit services rpm bgp]
user@host# set probe-type tcp-ping
```



**NOTE:** If you do not specify the probe type the default ICMP probes are sent.

8. Set the test interval.

```
[edit services rpm bgp]
user@host# set test-interval 60
```

**Results** From configuration mode, confirm your configuration by entering the **show services rpm** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show services rpm
bgp {
 probe-type tcp-ping;
 probe-count 5;
 probe-interval 1;
 test-interval 60;
 destination-port 50000;
 history-size 25;
 data-size 1024;
 data-fill ABCD123;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying RPM Probes for BGP Monitoring

---

**Purpose** Confirm that the configuration is working properly.

Verify that the RPM probes for BGP monitoring is configured.

**Action** From configuration mode, enter the **show services rpm** command.

- Related Documentation**
- [RPM Overview on page 1715](#)
  - [RPM Configuration Options on page 1732](#)
  - [Directing RPM Probes to Select BGP Devices on page 1730](#)
  - [Tuning RPM Probes on page 1732](#)

## Directing RPM Probes to Select BGP Devices

---

If a device has a large number of BGP neighbors configured, you can direct (filter) the RPM probes to a selected group of BGP neighbors rather than to all the neighbors. To identify the BGP devices to receive RPM probes, you can configure routing instances.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To direct RPM probes to select BGP neighbors:

1. Configure routing instance **R11** to send RPM probes to BGP neighbors within the routing instance.

```
[edit services rpm bgp]
user@host# set routing-instances R11
```

2. If you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [RPM Overview on page 1715](#)
- [RPM Configuration Options on page 1732](#)
- [Example: Configuring Basic RPM Probes on page 1721](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1728](#)
- [Tuning RPM Probes on page 1732](#)

## Configuring IPv6 RPM Probes

You can configure IPv6 source and destination addresses for an IPv6-based RPM probe test.

To configure an IPv6 RPM test:

1. Specify the RPM probe owner for the probe you want to configure as an IPv6 test.

```
[edit services rpm]
user@host# edit probe customerA
```

2. Specify a name for the test.

```
[edit services rpm probe customerA]
user@host# edit test ipv6-test
```

3. Specify the probe type.

```
[edit services rpm probe customerA test ipv6-test]
user@host# set probe-type icmp6-ping
```

4. Specify the source address for the test.

```
[edit services rpm probe customerA test ipv6-test]
user@host# set source-address 2001:db8:1a:1112::20
```

5. Specify the target address for the test.

```
[edit services rpm probe customerA test ipv6-test]
user@host# set target inet6-address 2001:db8:1a:1112::1
```

6. Configure the remaining RPM test parameters.

- Related Documentation**
- [Guidelines for Configuring RPM Probes for IPv6 on page 1719](#)

## Tuning RPM Probes

---

After configuring an RPM probe, you can set parameters to control probe functions, such as the interval between probes, the total number of concurrent probes that a system can handle, and the source address used for each probe packet. See [“Example: Configuring Basic RPM Probes” on page 1721](#).

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To tune RPM probes:

1. Set the maximum number of concurrent probes allowed on the system to **10**.

```
[edit services rpm]
user@host# set probe-limit 10
```

2. Access the ICMP probe of customer A.

```
[edit]
user@host# edit services rpm probe customerA test icmp-test
```

3. Set the time between probe transmissions to 15 seconds.

```
[edit services rpm probe customerA test icmp-test]
user@host# set probe-interval 15
```

4. Set the number of probes within a test to **10**.

```
[edit services rpm probe customerA test icmp-test]
user@host# set probe-count 10
```

5. Set the source address for each probe packet to **192.168.2.9**. If you do not explicitly configure a source address, the address on the outgoing interface through which the probe is sent is used as the source address.

```
[edit services rpm probe customerA test icmp-test]
user@host# set source-address 192.168.2.9
```

6. If you are done configuring the device, enter **commit** from configuration mode.

- Related Documentation**
- [RPM Overview on page 1715](#)
  - [RPM Configuration Options on page 1732](#)
  - [Example: Configuring RPM Probes for BGP Monitoring on page 1728](#)

## RPM Configuration Options

---

You can configure real-time performance monitoring (RPM) parameters. See [Table 143](#) for a summary of the configuration options.

Table 143: RPM Configuration Summary

| Field                              | Function                                                                                                                                                                                                        | Your Action                                                                                                                                                                                                                                                                                               |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Performance Probe Owners</b>    |                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                           |
| Owner Name (required)              | Identifies an RPM owner for which one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run (a particular customer, for example). | Type the name of the RPM owner.                                                                                                                                                                                                                                                                           |
| <b>Identification</b>              |                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                           |
| Test name (required)               | Uniquely identifies the RPM test                                                                                                                                                                                | Type the name of the RPM test.                                                                                                                                                                                                                                                                            |
| Target (Address or URL) (required) | IPv4 or IPv6 address or URL of probe target                                                                                                                                                                     | Type the IPv4 address, in dotted decimal notation, IPv6 address, or the URL of the probe target. If the target is a URL, type a fully formed URL that includes <b>http://</b> .                                                                                                                           |
| Source Address                     | Explicitly configured IPv4 or IPv6 address to be used as the probe source address                                                                                                                               | Type the source address to be used for the probe. If the source address is not one of the device's assigned addresses, the packet uses the outgoing interface's address as its source.                                                                                                                    |
| Routing Instance                   | Particular routing instance over which the probe is sent                                                                                                                                                        | Type the routing instance name. The routing instance applies only to probes of type <b>icmp</b> , <b>icmp6-ping</b> , and <b>icmp-timestamp</b> . The default routing instance is <b>inet.0</b> .                                                                                                         |
| History Size                       | Number of probe results saved in the probe history                                                                                                                                                              | Type a number between 0 and 255. The default history size is 50 probes.                                                                                                                                                                                                                                   |
| <b>Request Information</b>         |                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                           |
| Probe Type (required)              | Specifies the type of probe to send as part of the test.                                                                                                                                                        | Select the desired probe type from the list: <ul style="list-style-type: none"> <li>• <b>http-get</b></li> <li>• <b>http-get-metadata</b></li> <li>• <b>icmp6-ping</b></li> <li>• <b>icmp-ping</b></li> <li>• <b>icmp-ping-timestamp</b></li> <li>• <b>tcp-ping</b></li> <li>• <b>udp-ping</b></li> </ul> |
| Interval                           | Sets the wait time (in seconds) between each probe transmission                                                                                                                                                 | Type a number between 1 and 255 (seconds).                                                                                                                                                                                                                                                                |
| Test Interval (required)           | Sets the wait time (in seconds) between tests.                                                                                                                                                                  | Type a number between 0 and 86400 (seconds).                                                                                                                                                                                                                                                              |
| Probe Count                        | Sets the total number of probes to be sent for each test.                                                                                                                                                       | Type a number between 1 and 15.                                                                                                                                                                                                                                                                           |

Table 143: RPM Configuration Summary (*continued*)

| Field                           | Function                                                                                                                                                                                                                                                                                                                                                                      | Your Action                                                                                    |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Destination Port                | <p>Specifies the TCP or UDP port to which probes are sent.</p> <p>To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks devices configured to receive and transmit RPM probes on the same TCP or UDP port.</p>                                                             | Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535. |
| DSCP Bits                       | <p>Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is <b>000000</b>.</p>                                                                                                                                                                                                                                  | Type a valid 6-bit pattern.                                                                    |
| Data Size                       | Specifies the size of the data portion of the ICMP probes.                                                                                                                                                                                                                                                                                                                    | Type a size (in bytes) between 0 and 65507.                                                    |
| Data Fill                       | Specifies the contents of the data portion of the ICMP probes.                                                                                                                                                                                                                                                                                                                | Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.     |
| Hardware Timestamp              | <p>Enables timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter:</p> <ul style="list-style-type: none"> <li>• ICMP ping</li> <li>• ICMP ping timestamp</li> <li>• UDP ping—destination port UDP-ECHO (port 7) only</li> <li>• UDP ping timestamp—destination port UDP-ECHO (port 7) only</li> </ul> | To enable timestamping, select the check box.                                                  |
| <b>Maximum Probe Thresholds</b> |                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                |
| Successive Lost Probes          | Sets the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.                                                                                                                                                                                                                                                  | Type a number between 0 and 15.                                                                |
| Lost Probes                     | Sets the total number of probes that must be lost to trigger a probe failure and generate a system log message.                                                                                                                                                                                                                                                               | Type a number between 0 and 15.                                                                |
| Round Trip Time                 | Sets the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.                                                                                                                                                                                                                     | Type a number between 0 and 60,000,000 (microseconds).                                         |
| Jitter                          | Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.                                                                                                                                                                                                                                                        | Type a number between 0 and 60,000,000 (microseconds).                                         |
| Standard Deviation              | Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.                                                                                                                                                                                                                  | Type a number between 0 and 60,000,000 (microseconds).                                         |

Table 143: RPM Configuration Summary (*continued*)

| Field                               | Function                                                                                                                                                                       | Your Action                                                                                                                                                           |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Egress Time                         | Sets the total one-way time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.                         | Type a number between 0 and 60,000,000 (microseconds).                                                                                                                |
| Ingress Time                        | Sets the total one-way time (in microseconds), from the remote server to the device, that triggers a probe failure and generates a system log message.                         | Type a number between 0 and 60,000,000 (microseconds)                                                                                                                 |
| Jitter Egress Time                  | Sets the total outbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.                                           | Type a number between 0 and 60,000,000 (microseconds)                                                                                                                 |
| Jitter Ingress Time                 | Sets the total inbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.                                            | Type a number between 0 and 60,000,000 (microseconds).                                                                                                                |
| Egress Standard Deviation           | Sets the maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message. | Type a number between 0 and 60,000,000 (microseconds).                                                                                                                |
| Ingress Standard Deviation          | Sets the maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.  | Type a number between 0 and 60,000,000 (microseconds).                                                                                                                |
| <b>Traps</b>                        |                                                                                                                                                                                |                                                                                                                                                                       |
| Egress Jitter Exceeded              | Generates SNMP traps when the threshold for jitter in outbound time is exceeded.                                                                                               | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Egress Standard Deviation Exceeded  | Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.                                                                                  | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Egress Time Exceeded                | Generates SNMP traps when the threshold for maximum outbound time is exceeded.                                                                                                 | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Ingress Jitter Exceeded             | Generates SNMP traps when the threshold for jitter in inbound time is exceeded.                                                                                                | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Ingress Standard Deviation Exceeded | Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.                                                                                   | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Ingress Time Exceeded               | Generates traps when the threshold for maximum inbound time is exceeded.                                                                                                       | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |

Table 143: RPM Configuration Summary (*continued*)

| Field                           | Function                                                                                   | Your Action                                                                                                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jitter Exceeded                 | Generates traps when the threshold for jitter in round-trip time is exceeded.              | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Probe Failure                   | Generates traps when the threshold for the number of successive lost probes is reached.    | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| RTT Exceeded                    | Generates traps when the threshold for maximum round-trip time is exceeded.                | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Standard Deviation Exceeded     | Generates traps when the threshold for standard deviation in round-trip times is exceeded. | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Test Completion                 | Generates traps when a test is completed.                                                  | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Test Failure                    | Generates traps when the threshold for the total number of lost probes is reached.         | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| <b>Performance Probe Server</b> |                                                                                            |                                                                                                                                                                       |
| TCP Probe Server                | Specifies the port on which the device is to receive and transmit TCP probes.              | Type the number 7—a standard TCP or UDP port number—or a port number from 49160 through 65535.                                                                        |
| UDP Probe Server                | Specifies the port on which the device is to receive and transmit UDP probes.              | Type the number 7—a standard TCP or UDP port number—or a port number from 49160 through 65535.                                                                        |

- Related Documentation**
- [RPM Overview on page 1715](#)
  - [Example: Configuring Basic RPM Probes on page 1721](#)
  - [Example: Configuring RPM Using TCP and UDP Probes on page 1725](#)
  - [Example: Configuring RPM Probes for BGP Monitoring on page 1728](#)

## Monitoring RPM Probes

The RPM information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the device. To view these RPM properties, select **Troubleshoot > RPM > View RPM** in the J-Web user interface, or in configuration mode enter the **show** command:

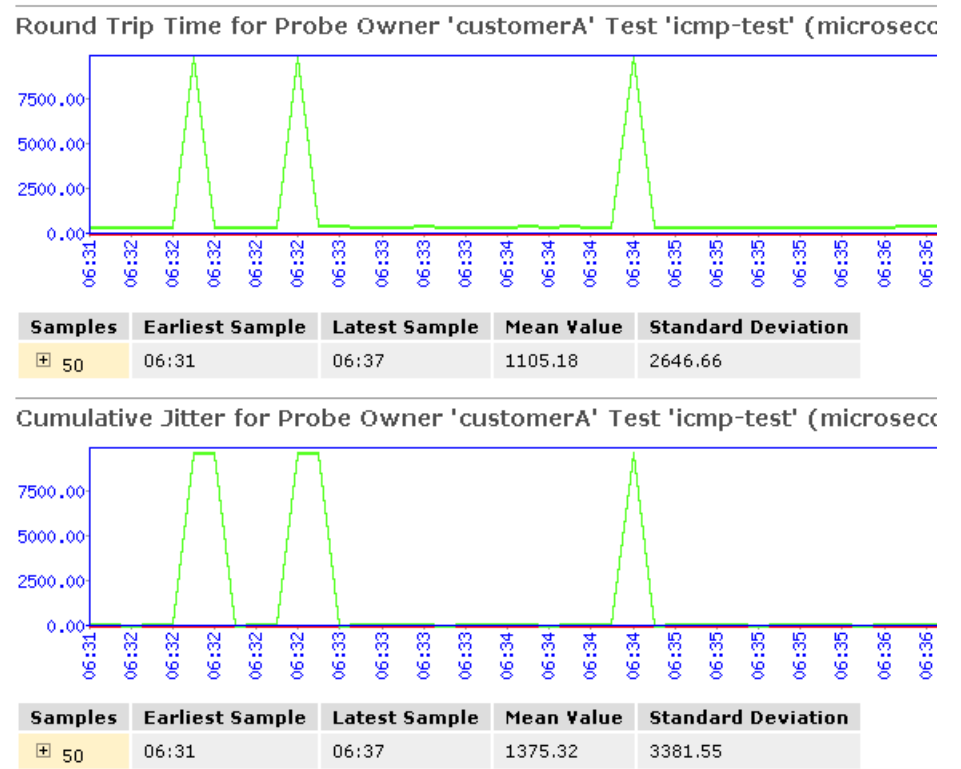
[edit]



```
user@host# run show services rpm probe-results
```

In addition to the RPM statistics for each RPM test, the J-Web user interface displays the round-trip times and cumulative jitter graphically. Figure 40 shows sample graphs for an RPM test.

Figure 40: Sample RPM Graphs



In Figure 40, the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Table 144 summarizes key output fields in RPM displays.

Table 144: Summary of Key RPM Output Fields

| Field                   | Values                                 | Additional Information                                                                                                          |
|-------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Currently Running Tests |                                        |                                                                                                                                 |
| Graph                   |                                        | Click the <b>Graph</b> link to display the graph (if it is not already displayed) or to update the graph for a particular test. |
| Owner                   | Configured owner name of the RPM test. | —                                                                                                                               |
| Test Name               | Configured name of the RPM test.       | —                                                                                                                               |

Table 144: Summary of Key RPM Output Fields (*continued*)

| Field                              | Values                                                                                                                                                                                                                                                                                                            | Additional Information                                                                                                                                                          |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probe Type                         | Type of RPM probe configured for the specified test: <ul style="list-style-type: none"> <li>• <b>http-get</b></li> <li>• <b>http-get-metadata</b></li> <li>• <b>icmp-ping</b></li> <li>• <b>icmp6-ping</b></li> <li>• <b>icmp-ping-timestamp</b></li> <li>• <b>tcp-ping</b></li> <li>• <b>udp-ping</b></li> </ul> | —                                                                                                                                                                               |
| Target Address                     | IPv4 address, IPv6 address, or URL of the remote server that is being probed by the RPM test.                                                                                                                                                                                                                     | —                                                                                                                                                                               |
| Source Address                     | Explicitly configured IPv4 or IPv6 source address that is included in the probe packet headers.                                                                                                                                                                                                                   | If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.                              |
| Minimum RTT                        | Shortest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.                                                                                                                                                                                          | —                                                                                                                                                                               |
| Maximum RTT                        | Longest round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.                                                                                                                                                                                           | —                                                                                                                                                                               |
| Average RTT                        | Average round-trip time from the Juniper Networks device to the remote server, as measured over the course of the test.                                                                                                                                                                                           | —                                                                                                                                                                               |
| Standard Deviation RTT             | Standard deviation of round-trip times from the Juniper Networks device to the remote server, as measured over the course of the test.                                                                                                                                                                            | —                                                                                                                                                                               |
| Probes Sent                        | Total number of probes sent over the course of the test.                                                                                                                                                                                                                                                          | —                                                                                                                                                                               |
| Loss Percentage                    | Percentage of probes sent for which a response was not received.                                                                                                                                                                                                                                                  | —                                                                                                                                                                               |
| <b>Round-Trip Time for a Probe</b> |                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                 |
| Samples                            | Total number of probes used for the data set.                                                                                                                                                                                                                                                                     | The Juniper Networks device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test. |
| Earliest Sample                    | System time when the first probe in the sample was received.                                                                                                                                                                                                                                                      | —                                                                                                                                                                               |
| Latest Sample                      | System time when the last probe in the sample was received.                                                                                                                                                                                                                                                       | —                                                                                                                                                                               |

Table 144: Summary of Key RPM Output Fields (*continued*)

| Field                                | Values                                                                                                               | Additional Information                                                                                                                                                          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mean Value                           | Average round-trip time for the 50-probe sample.                                                                     | –                                                                                                                                                                               |
| Standard Deviation                   | Standard deviation of the round-trip times for the 50-probe sample.                                                  | –                                                                                                                                                                               |
| Lowest Value                         | Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.                 | –                                                                                                                                                                               |
| Time of Lowest Sample                | System time when the lowest value in the 50-probe sample was received.                                               | –                                                                                                                                                                               |
| Highest Value                        | Longest round-trip time from the Juniper Networks device to the remote server, as measured over the 50-probe sample. | –                                                                                                                                                                               |
| Time of Highest Sample               | System time when the highest value in the 50-probe sample was received.                                              | –                                                                                                                                                                               |
| <b>Cumulative Jitter for a Probe</b> |                                                                                                                      |                                                                                                                                                                                 |
| Samples                              | Total number of probes used for the data set.                                                                        | The Juniper Networks device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test. |
| Earliest Sample                      | System time when the first probe in the sample was received.                                                         | –                                                                                                                                                                               |
| Latest Sample                        | System time when the last probe in the sample was received.                                                          | –                                                                                                                                                                               |
| Mean Value                           | Average jitter for the 50-probe sample.                                                                              | –                                                                                                                                                                               |
| Standard Deviation                   | Standard deviation of the jitter values for the 50-probe sample.                                                     | –                                                                                                                                                                               |
| Lowest Value                         | Smallest jitter value, as measured over the 50-probe sample.                                                         | –                                                                                                                                                                               |
| Time of Lowest Sample                | System time when the lowest value in the 50-probe sample was received.                                               | –                                                                                                                                                                               |
| Highest Value                        | Highest jitter value, as measured over the 50-probe sample.                                                          | –                                                                                                                                                                               |
| Time of Highest Sample               | System time when the highest jitter value in the 50-probe sample was received.                                       | –                                                                                                                                                                               |

- Related Documentation**
- [RPM Overview on page 1715](#)
  - [RPM Support for VPN Routing and Forwarding on page 1721](#)
  - [RPM Configuration Options on page 1732](#)

# Configuring IP Monitoring

- [IP Monitoring Overview on page 1741](#)
- [Understanding IP Monitoring Test Parameters on page 1742](#)
- [Example: Configuring IP Monitoring on Branch SRX Series Devices on page 1743](#)
- [Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups on page 1745](#)
- [Example: Configuring IP Monitoring on High-End SRX Series Devices on page 1746](#)
- [Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring on page 1751](#)

## IP Monitoring Overview

---

This feature monitors IP on standalone SRX Series devices or a chassis cluster redundant Ethernet (reth) interface. Existing RPM probes are sent to an IP address to check for reachability. The user takes action based on the reachability result. Supported action currently is preferred static route injection to system route table.

The actions supported are:

- Adding or deleting a new static route that has a higher priority (lower preference) value than a route configured through the CLI command **set routing-options static route**
- Defining multiple probe names under the same IP monitoring policy. If any probe fails, the action is taken. If all probes are reachable, the action is reverted
- Configuring multiple tests in one RPM probe. All tests must fail for the RPM probe to be considered unreachable. If at least one test reaches its target, the RPM probe is considered reachable
- Configuring multiple failure thresholds in one RPM test. If one threshold is reached, the test fails. If no thresholds are reached, the test succeeds.
- Specifying the no-preempt option. If the no-preempt option is specified, the policy does not perform preemptive failback when it is in a failover state or when the RPM probe test recovers from a failure.
- Setting preferred metric values. If the preferred metric value is set, during failover, the route is injected with the set preferred metric value.
- Enabling and disabling interfaces.

- **Interface-Enable**—On a physical or logical interface, when the interface-enable action is configured, the initial state of the interface is disable after startup, and it continues to remain in the disable state as long as the associated RPM probe is in the pass state. When the associated RPM probe fails, the configured physical and logical interfaces are enabled.
- **Interface-Disable**—On a physical or logical interface, when the interface-disable action is configured, the interface state remains unchanged. When the associated RPM probe fails, the physical and logical interfaces are disabled.



**NOTE:** Multiple probe names and actions can be defined for the same IP monitoring policy.

**Related  
Documentation**

- [Understanding IP Monitoring Test Parameters on page 1742](#)

## Understanding IP Monitoring Test Parameters

Each probed target is monitored over the course of a test, which represents a collection of probes during which statistics such as standard deviation and jitter are collected are calculated. During a test, probes are generated and responses collected at a rate defined by the probe interval, the number of seconds between probes.



**NOTE:** To avoid flap, an action is reverted only at the end of a test cycle. During the test cycle, if no threshold is reached, the action is reverted. Although action-failover takes place based on a predefined condition of a monitored IP, when the condition is reversed, the IP becomes reachable on the original route, and the newly added route is deleted. Recovery is performed only when all RPM probes report the IP as reachable.

Table 145 lists the test parameters and its default values:

**Table 145: Test Parameters and Default Values**

| Parameter      | Default Value |
|----------------|---------------|
| probe-count    | 1             |
| probe-interval | 3 seconds     |
| test-interval  | 1 second      |

Table 146 lists the supported threshold and its description:

Table 146: Threshold Supported and Description

| Threshold       | Description                     |
|-----------------|---------------------------------|
| Successive-Loss | Successive loss count of probes |
| Total-Loss      | Total probe lost count          |

**Related Documentation**

- [IP Monitoring Overview on page 1741](#)

## Example: Configuring IP Monitoring on Branch SRX Series Devices

This example shows how to monitor IP on branch SRX Series devices.

- [Requirements on page 1743](#)
- [Overview on page 1743](#)
- [Configuration on page 1743](#)
- [Verification on page 1745](#)

### Requirements

Before you begin:

Configure the following RPM options for RPM test:

- target-address
- probe-count
- probe-interval
- test-interval
- thresholds
- next-hop

### Overview

This example shows how to set up IP monitoring on an SRX Series for the branch device.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set services rpm probe Probe-Payment-Server test paysvr target address 1.1.1.10
set services rpm probe Probe-Payment-Server test paysvr probe-count 10
set services rpm probe Probe-Payment-Server test paysvr probe-interval 5
set services rpm probe Probe-Payment-Server test paysvr test-interval 5
set services rpm probe Probe-Payment-Server test paysvr thresholds successive-loss 10
```

```

set services rpm probe Probe-Payment-Server test paysvr next-hop 2.2.2.1
set services ip-monitoring policy Payment-Server-Tracking match rpm-probe
Probe-Payment-Server
set services ip-monitoring policy Payment-Server-Tracking then preferred-route route
1.1.1.0/24 next-hop 1.1.1.99

```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure IP monitoring on an SRX Series Services Gateway:

1. Configure the target address under the RPM probe.  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr target address
1.1.1.10

```
2. Configure the probe count under the RPM probe.  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-count
10

```
3. Configure the probe interval (in seconds) under the RPM probe.  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-interval
5

```
4. Configure the test interval (in seconds) under the RPM probe.  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr test-interval
5

```
5. Configure the threshold successive loss count under the RPM  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr thresholds
successive-loss 10

```
6. Configure the next-hop IP address under the RPM probe.  

```

[edit]
user@host# set services rpm probe Probe-Payment-Server test paysvr next-hop
2.2.2.1

```
7. Configure the IP monitoring policy under services.  

```

[edit]
user@host# set services ip-monitoring policy Payment-Server-Tracking match
rpm-probe Probe-Payment-Server

```



**NOTE:** The following steps are not mandatory. You can configure interface actions and route actions independently, or you can configure both the interface action and the route action together in one IP monitoring policy.



8. Configure the IP monitoring preferred route under services.

```
[edit]
user@host# set services ip-monitoring policy Payment-Server-Tracking then
preferred-route route 1.1.1.0/24 preferred-metric 4
```

9. Configure the IP monitoring interface actions.

- Enable

```
[edit]
user@host# set services ip-monitoring policy Payment-Server-Tracking then
interface ge-0/0/1 enable
```

- Disable

```
[edit]
user@host# set services ip-monitoring policy Payment-Server-Tracking then
interface fe-0/0/[4-6] disable
```

10. Configure the no-preempt option.

```
[edit]
user@host# set services ip-monitoring policy Payment-Server-Tracking no-preempt
```

## Verification

### Verifying IP Monitoring

**Purpose** Verify the IP monitoring status of a policy.

**Action** To verify the configuration is working properly, enter the following command:

```
show services ip-monitoring status <policy-name>
```

**Related Documentation**

- [IP Monitoring Overview on page 1741](#)
- [Understanding IP Monitoring Test Parameters on page 1742](#)

## Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups

IP monitoring checks the reachability of an upstream device. It is designed to check the end-to-end connectivity of configured IP addresses and allows a redundancy group (RG) to automatically failover when the monitored IP address is not reachable through the redundant Ethernet. Both the primary and secondary devices in the chassis cluster monitor specific IP addresses to determine whether an upstream device in the network is reachable.

A redundant Ethernet interface contains physical interfaces from both the primary and secondary nodes in the SRX Series chassis cluster. In a redundant Ethernet interface, two physical interfaces are configured with each node contributing one physical interface. In a redundant Ethernet interface LAG, more than two physical interfaces are configured in the redundant Ethernet interface.

- Related Documentation**
- [IP Monitoring Overview on page 1741](#)

---

## Example: Configuring IP Monitoring on High-End SRX Series Devices

---

This example shows how to monitor IP on a high-end SRX Series device with chassis cluster enabled.

- [Requirements on page 1746](#)
- [Overview on page 1746](#)
- [Configuration on page 1747](#)
- [Verification on page 1749](#)

### Requirements

- You need two SRX5800 Services Gateways with identical hardware configurations, one SRX Series device and one EX8208 Ethernet Switch.
- Physically connect the two SRX5800 devices (back-to-back for the fabric and control ports) and ensure that they are the same models. Configure/add these two devices in a cluster.

### Overview

IP address monitoring checks end-to-end reachability of configured IP address and allows a redundancy group to automatically fail over when not reachable through the child link of redundant Ethernet interface (known as a reth) interface. Redundancy groups on both devices in a cluster can be configured to monitor specific IP addresses to determine whether an upstream device in the network is reachable.

This example shows how to set up IP monitoring on a high-end SRX Series device.



NOTE: IP monitoring is not supported on an NP-IOC card.

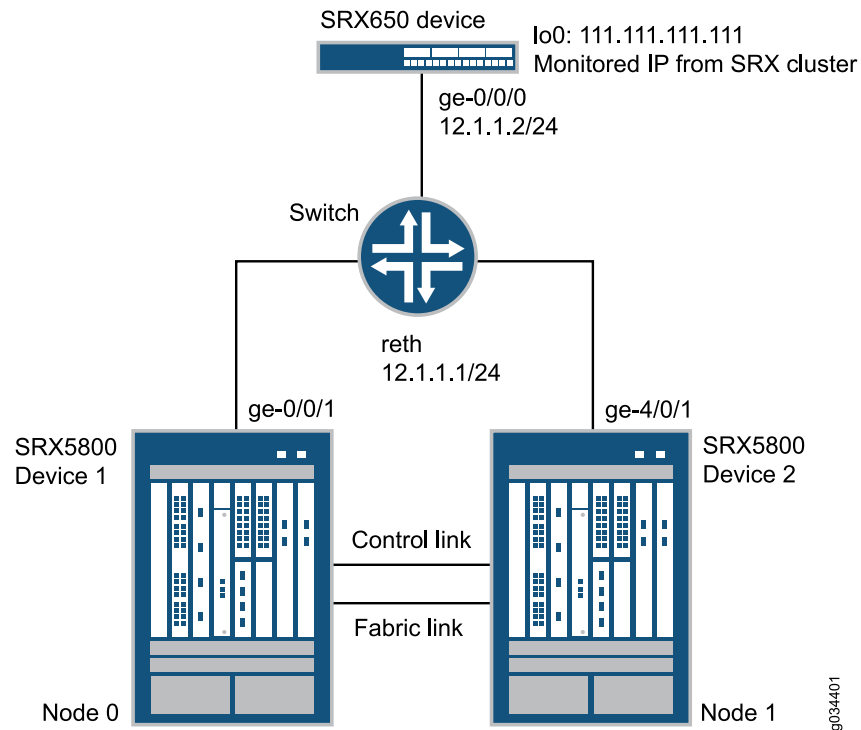
---

### Topology

---

Figure 41 shows the topology used in this example.

**Figure 41: IP Monitoring on a High-End SRX Series Device Topology Example**



In this example, two SRX5800 devices in a chassis cluster are connected to an SRX650 device through an EX8208 Ethernet Switch. The example shows how the redundancy groups can be configured to monitor key upstream resources reachable through redundant Ethernet interfaces on either node in a cluster.

## Configuration

- [Configuring IP Monitoring on a High-End SRX Series Device on page 1748](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set chassis cluster reth-count 1
set chassis cluster redundancy-group 0 node 0 priority 254
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 199
set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 111.111.111.111
weight 80
set chassis cluster redundancy-group 1 ip-monitoring family inet 111.111.111.111
interface reth0.0 secondary-ip-address 12.1.1.3
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
```

```

set interfaces ge-4/0/1 gigether-options redundant-parent reth0
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 12.1.1.1/24
set routing-options static route 111.111.111.111/32 next-hop 12.1.1.2

```

### Configuring IP Monitoring on a High-End SRX Series Device

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure IP monitoring on a high-end SRX Series device:

1. Specify the number of redundant Ethernet interfaces.  

```

{primary:node0}[edit]
user@host# set chassis cluster reth-count 1

```
2. Specify a redundancy group's priority for primacy on each node of the cluster. The higher number takes precedence.  

```

{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# set chassis cluster redundancy-group 1 node 0 priority 200
user@host# set chassis cluster redundancy-group 1 node 1 priority 199

```
3. Configure the redundant Ethernet interfaces to redundancy-group 1.  

```

{primary:node0}[edit]
user@host# set interfaces reth0 redundant-ether-options redundancy-group 1
user@host# set interfaces reth0 unit 0 family inet address 12.1.1.1/24

```
4. Assign child interfaces for the redundant Ethernet interfaces from node 0 and node 1.  

```

{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth0
user@host# set interfaces ge-4/0/1 gigether-options redundant-parent reth0

```
5. Configure the static route to the IP address that is to be monitored.  

```

{primary:node0}[edit]
user@host# set routing-options static route 111.111.111.111/32 next-hop 12.1.1.2

```
6. Configure IP monitoring under redundancy-group 1 with global weight and global threshold.  

```

{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80

```
7. Specify the retry interval.  

```

{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3

```
8. Specify the retry count.  

```

{primary:node0}[edit]

```

```
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

9. Assign a weight to the IP address to be monitored, and configure a secondary IP address that will be used to send ICMP packets from the secondary node to track the IP being monitored.

```
{primary:node0}[edit]
```

```
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet
111.111.111.111 weight 80
```

```
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet
111.111.111.111 interface reth0.0 secondary-ip-address 12.1.1.3
```



**NOTE:**

- The redundant Ethernet (reth0) IP address, 12.1.1.1/24, is used to send ICMP packets from node 0 to check the reachability of the monitored IP.
- The secondary IP address, 12.1.1.3, should belong to the same network as the reth0 IP address.
- The secondary IP address is used to send ICMP packets from node 1 to check the reachability of the monitored IP.

## Verification

Confirm the configuration is working properly.

- [Verifying Chassis Cluster Status—Before Failover on page 1749](#)
- [Verifying Chassis Cluster IP Monitoring Status—Before Failover on page 1750](#)
- [Verifying Chassis Cluster Status—After Failover on page 1750](#)
- [Verifying Chassis Cluster IP Monitoring Status—After Failover on page 1751](#)

### Verifying Chassis Cluster Status—Before Failover

**Purpose** Verify the chassis cluster status, failover status, and redundancy group information before failover.

**Action** From operational mode, enter the **show chassis cluster status** command.

```
show chassis cluster status
```

Cluster ID: 11

| Node | Priority | Status | Preempt | Manual failover |
|------|----------|--------|---------|-----------------|
|------|----------|--------|---------|-----------------|

Redundancy group: 0 , Failover count: 0

|       |     |           |    |    |
|-------|-----|-----------|----|----|
| node0 | 254 | primary   | no | no |
| node1 | 1   | secondary | no | no |

Redundancy group: 1 , Failover count: 0

|       |     |           |    |    |
|-------|-----|-----------|----|----|
| node0 | 200 | primary   | no | no |
| node1 | 199 | secondary | no | no |

### Verifying Chassis Cluster IP Monitoring Status—Before Failover

**Purpose** Verify the IP status being monitored from both nodes and the failover count for both nodes before failover.

**Action** From operational mode, enter the **show chassis cluster ip-monitoring status redundancy-group 1** command.

```
show chassis cluster ip-monitoring status redundancy-group 1
```

node0:

-----

Redundancy group: 1

| IP address      | Status    | Failure count | Reason |
|-----------------|-----------|---------------|--------|
| 111.111.111.111 | reachable | 0             | n/a    |

node1:

-----

Redundancy group: 1

| IP address      | Status    | Failure count | Reason |
|-----------------|-----------|---------------|--------|
| 111.111.111.111 | reachable | 0             | n/a    |

### Verifying Chassis Cluster Status—After Failover

**Purpose** Verify the chassis cluster status, failover status, and redundancy group information after failover.



**NOTE:** If the IP address is not reachable, the following output will be displayed.

**Action** From operational mode, enter the **show chassis cluster status** command.

```
show chassis cluster status
```

```
Cluster ID: 11
Node Priority Status Preempt Manual failover

Redundancy group: 0 , Failover count: 0
 node0 254 primary no no
 node1 1 secondary no no

Redundancy group: 1 , Failover count: 1
 node0 0 secondary no no
 node1 199 primary no no
```

### Verifying Chassis Cluster IP Monitoring Status—After Failover

**Purpose** Verify the IP status being monitored from both nodes and the failover count for both nodes after failover.

**Action** From operational mode, enter the **show chassis cluster ip-monitoring status redundancy-group 1** command.

```
show chassis cluster ip-monitoring status redundancy-group 1
```

```
node0:
```

```
Redundancy group: 1
```

| IP address      | Status      | Failure count | Reason  |
|-----------------|-------------|---------------|---------|
| 111.111.111.111 | unreachable | 1             | unknown |

```
node1:
```

```
Redundancy group: 1
```

| IP address      | Status    | Failure count | Reason |
|-----------------|-----------|---------------|--------|
| 111.111.111.111 | reachable | 0             | n/a    |

**Related Documentation**

- [Example: Configuring an Active/Passive Chassis Cluster On a High-End SRX Series Services Gateway](#)

## Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring

This example shows how to configure redundancy group IP address monitoring for an SRX Series device in a chassis cluster.

- [Requirements on page 1752](#)
- [Overview on page 1752](#)

- [Configuration on page 1753](#)
- [Verification on page 1754](#)

## Requirements

Before you begin:

- Set the chassis cluster node ID and cluster ID. See [Example: Setting the Chassis Cluster Node ID and Cluster ID for Branch SRX Series Devices](#) or [Example: Setting the Chassis Cluster Node ID and Cluster ID](#).
- Configure the chassis cluster management interface. See [Example: Configuring the Chassis Cluster Management Interface](#).
- Configure the chassis cluster fabric. See [Example: Configuring the Chassis Cluster Fabric Interfaces](#).

## Overview

You can configure redundancy groups to monitor upstream resources by pinging specific IP addresses that are reachable through redundant Ethernet interfaces on either node in a cluster. You can also configure global threshold, weight, retry interval, and retry count parameters for a redundancy group. When a monitored IP address becomes unreachable, the weight of that monitored IP address is deducted from the redundancy group IP address monitoring global threshold. When the global threshold reaches 0, the global weight is deducted from the redundancy group threshold. The retry interval determines the ping interval for each IP address monitored by the redundancy group. The pings are sent as soon as the configuration is committed. The retry count sets the number of allowed consecutive ping failures for each IP address monitored by the redundancy group.

In this example, you configure the following settings for redundancy group 1:

- IP address to monitor—10.1.1.10
- IP address monitoring global-weight—100
- IP address monitoring global-threshold—200



**NOTE:** The threshold applies cumulatively to all IP addresses monitored by the redundancy group.

---

- IP address retry-interval—3 seconds
- IP address retry-count—10
- Weight—150
- Redundant Ethernet interface—reth1.0
- Secondary IP address—10.1.1.101



## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
{primary:node0}[edit]
user@host#
set chassis cluster redundancy-group 1 ip-monitoring global-weight 100
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 200
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10 weight 150
interface reth1.0 secondary-ip-address 10.1.1.101
```

**Step-by-Step Procedure** To configure redundancy group IP address monitoring:

1. Specify a global monitoring weight.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight
100
```

2. Specify the global monitoring threshold.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold
200
```

3. Specify the retry interval.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
```

4. Specify the retry count.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

5. Specify the IP address to be monitored, weight, redundant Ethernet interface, and secondary IP address.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10
weight 100 interface reth1.0 secondary-ip-address 10.1.1.101
```

**Results** From configuration mode, confirm your configuration by entering the **show chassis cluster redundancy-group 1** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
{primary:node0}[edit]
user@host# show chassis cluster redundancy-group 1
ip-monitoring {
 global-weight 100;
 global-threshold 200;
 family {
```

```

 inet {
 10.1.1.10 {
 weight 100;
 interface reth1.0 secondary-ip-address 10.1.1.101;
 }
 }
 }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying the Status of Monitored IP Addresses for a Redundancy Group

**Purpose** Verify the status of monitored IP addresses for a redundancy group.

**Action** From operational mode, enter the **show chassis cluster ip-monitoring status** command. For information about a specific group, enter the **show chassis cluster ip-monitoring status redundancy-group** command.

```

{primary:node0}
user@host> show chassis cluster ip-monitoring status
node0:

```

```

Redundancy group: 1
Global threshold: 200
Current threshold: -120

```

| IP address | Status    | Failure count | Reason | Weight |
|------------|-----------|---------------|--------|--------|
| 10.1.1.10  | reachable | 0             | n/a    | 220    |
| 10.1.1.101 | reachable | 0             | n/a    | 100    |

```

node1:

```

```

Redundancy group: 1
Global threshold: 200
Current threshold: -120

```

| IP address | Status    | Failure count | Reason | Weight |
|------------|-----------|---------------|--------|--------|
| 10.1.1.10  | reachable | 0             | n/a    | 220    |
| 10.1.1.101 | reachable | 0             | n/a    | 100    |

**Related Documentation**

- [Understanding Chassis Cluster Redundancy Group Interface Monitoring](#)

## PART 22

# Monitoring Common Security Features

- [Displaying Real-Time Information from Device to Host on page 1757](#)
- [Monitoring Application Layer Gateways Features on page 1763](#)
- [Monitoring Interfaces and Switching Functions on page 1789](#)
- [Monitoring NAT on page 1807](#)
- [Monitoring Security Policies on page 1819](#)
- [Monitoring Events, Services and System on page 1845](#)
- [Monitoring Unified Threat Management Features on page 1855](#)
- [Monitoring VPNs on page 1867](#)



# Displaying Real-Time Information from Device to Host

- [Displaying Real-Time Monitoring Information on page 1757](#)
- [Displaying Multicast Path Information on page 1759](#)

## Displaying Real-Time Monitoring Information

To display real-time monitoring information about each device between the device and a specified destination host, enter the **traceroute monitor** command with the following syntax:

```
user@host> traceroute monitor host <count number> <inet | inet6> <interval seconds>
<no-resolve> <size bytes> <source source-address> <summary>
```

[Table 147](#) describes the **traceroute monitor** command options.

**Table 147: CLI traceroute monitor Command Options**

| Option                  | Description                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host</i>             | Sends traceroute packets to the hostname or IP address you specify.                                                                                                       |
| <i>count number</i>     | (Optional) Limits the number of ping requests, in packets, to send in summary mode. If you do not specify a count, ping requests are continuously sent until you press Q. |
| <i>inet</i>             | (Optional) Forces the traceroute packets to an IPv4 destination.                                                                                                          |
| <i>inet6</i>            | (Optional) Forces the traceroute packets to an IPv6 destination.                                                                                                          |
| <i>interval seconds</i> | (Optional) Sets the interval between ping requests, in seconds. The default value is 1 second.                                                                            |
| <i>no-resolve</i>       | (Optional) Suppresses the display of the hostnames of the hops along the path.                                                                                            |
| <i>size bytes</i>       | (Optional) Sets the size of the ping request packet. The size can be from 0 through 65,468 bytes. The default packet size is 64 bytes.                                    |
| <i>source address</i>   | (Optional) Uses the source address that you specify, in the traceroute packet.                                                                                            |
| <i>summary</i>          | (Optional) Displays the summary traceroute information.                                                                                                                   |

To quit the **traceroute monitor** command, press Q.

The following is sample output from a **traceroute monitor** command:

```

user@host> traceroute monitor host2

My traceroute [v0.69]
host (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)
 Wed Mar 14 23:14:11 2007
Keys: Help Display mode Restart statistics Order of fields quit

 Pings
Host
Last Avg Best Wrst StDev
1. 173.24.232.66 0.0% 5
9.4 8.6 4.8 9.9 2.1
2. 173.24.232.66 0.0% 5
7.9 17.2 7.9 29.4 11.0
3. 173.24.232.66 0.0% 5
9.9 9.3 8.7 9.9 0.5
4. 173.24.232.66 0.0% 5
9.9 9.8 9.5 10.0 0.2

```

Table 148 summarizes the output fields of the display.

**Table 148: CLI traceroute monitor Command Output Summary**

| Field                     | Description                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>host</b>               | Hostname or IP address of the device issuing the <b>traceroute monitor</b> command.                          |
| <b>psizesize</b>          | Size of ping request packet, in bytes.                                                                       |
| <b>Keys</b>               |                                                                                                              |
| <b>Help</b>               | Displays the Help for the CLI commands.<br>Press H to display the Help.                                      |
| <b>Display mode</b>       | Toggles the display mode.<br>Press D to toggle the display mode                                              |
| <b>Restart statistics</b> | Restarts the <b>traceroute monitor</b> command.<br>Press R to restart the <b>traceroute monitor</b> command. |
| <b>Order of fields</b>    | Sets the order of the displayed fields.<br>Press O to set the order of the displayed fields.                 |
| <b>quit</b>               | Quits the <b>traceroute monitor</b> command.<br>Press Q to quit the <b>traceroute monitor</b> command.       |
| <b>Packets</b>            |                                                                                                              |
| <b>number</b>             | Number of the hop (device) along the route to the final destination host.                                    |

Table 148: CLI traceroute monitor Command Output Summary (*continued*)

| Field | Description                                                                                                             |
|-------|-------------------------------------------------------------------------------------------------------------------------|
| Host  | Hostname or IP address of the device at each hop.                                                                       |
| Loss% | Percent of packet loss. The number of ping responses divided by the number of ping requests, specified as a percentage. |
| Pings |                                                                                                                         |
| Snt   | Number of ping requests sent to the device at this hop.                                                                 |
| Last  | Most recent round-trip time, in milliseconds, to the device at this hop.                                                |
| Avg   | Average round-trip time, in milliseconds, to the device at this hop.                                                    |
| Best  | Shortest round-trip time, in milliseconds, to the device at this hop.                                                   |
| Wrst  | Longest round-trip time, in milliseconds, to the device at this hop.                                                    |
| StDev | Standard deviation of round-trip times, in milliseconds, to the device at this hop.                                     |

Related Documentation • [Displaying Log and Trace Files on page 1900](#)

## Displaying Multicast Path Information

To display information about a multicast path from a source to the device, enter the **mtrace from-source** command with the following syntax:

```
user@host> mtrace from-source source host <extra-hops number> <group address>
<interval seconds> <max-hops number> <max-queries number> <response host>
<routing-instance routing-instance-name> <tll number> <wait-time seconds> <loop>
<multicast-response | unicast-response> <no-resolve> <no-router-alert> <brief |
detail>
```

Table 149 describes the **mtrace from-source** command options.

Table 149: CLI mtrace from-source Command Options

| Option                   | Description                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>source host</b>       | Traces the path to the specified hostname or IP address.                                                          |
| <b>extra-hops number</b> | (Optional) Sets the number of extra hops to trace past nonresponsive devices. Specify a value from 0 through 255. |
| <b>group address</b>     | (Optional) Traces the path for the specified group address. The default value is 192.0.2.0.                       |
| <b>interval seconds</b>  | (Optional) Sets the interval between statistics gathering. The default value is 10.                               |

Table 149: CLI mtrace from-source Command Options (*continued*)

| Option                                               | Description                                                                                                                                                                                                                                          |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>max-hops <i>number</i></b>                        | (Optional) Sets the maximum number of hops to trace toward the source. Specify a value from 0 through 255. The default value is 32.                                                                                                                  |
| <b>max-queries <i>number</i></b>                     | (Optional) Sets the maximum number of query attempts for any hop. Specify a value from 1 through 32. The default value is 3.                                                                                                                         |
| <b>response <i>host</i></b>                          | (Optional) Sends the response packets to the specified hostname or IP address. By default, the response packets are sent to the device.                                                                                                              |
| <b>routing-instance <i>routing-instance-name</i></b> | (Optional) Traces the routing instance you specify.                                                                                                                                                                                                  |
| <b>ttl <i>number</i></b>                             | (Optional) Sets the time-to-live (TTL) value in the IP header of the query packets. Specify a hop count from 0 through 255. The default value for local queries to the <b>all routers</b> multicast group is 1. Otherwise, the default value is 127. |
| <b>wait-time <i>seconds</i></b>                      | (Optional) Sets the time to wait for a response packet. The default value is 3 seconds.                                                                                                                                                              |
| <b>loop</b>                                          | (Optional) Loops indefinitely, displaying rate and loss statistics. To quit the <b>mtrace</b> command, press Ctrl-C.                                                                                                                                 |
| <b>multicast-response</b>                            | (Optional) Forces the responses to use multicast.                                                                                                                                                                                                    |
| <b>unicast-response</b>                              | (Optional) Forces the response packets to use unicast.                                                                                                                                                                                               |
| <b>no-resolve</b>                                    | (Optional) Does not display hostnames.                                                                                                                                                                                                               |
| <b>no-router-alert</b>                               | (Optional) Does not use the device alert IP option in the IP header.                                                                                                                                                                                 |
| <b>brief</b>                                         | (Optional) Does not display packet rates and losses.                                                                                                                                                                                                 |
| <b>detail</b>                                        | (Optional) Displays packet rates and losses if a group address is specified.                                                                                                                                                                         |

The following is sample output from the **mtrace from-source** command:

```

user@host> mtrace from-source source 192.1.4.1 group 224.1.1.1

Mtrace from 192.1.4.1 to 192.1.30.2 via group 224.1.1.1 Querying full reverse
path... * * 0 ? (192.1.30.2) -1 ? (192.1.30.1) PIM thresh^ 1 -2
routerC.mycompany.net (192.1.40.2) PIM thresh^ 1 -3 hostA.mycompany.net
(192.1.4.1) Round trip time 22 ms; total ttl of 2 required. Waiting to accumulate
statistics...Results after 10 seconds: Source Response Dest Overall
Packet Statistics For Traffic From 192.1.4.1 192.1.30.2 Packet
192.1.4.1 To 224.1.1.1 v ___/ rtt 16 ms Rate Lost/Sent =
Pct Rate 192.168.195.37 192.1.40.2 routerC.mycompany.net v ^
ttl 2 0/0 = -- 0 pps 192.1.40.1 192.1.30.1
? ? v ___ ttl 3 ?/0
0 pps 192.1.30.2 192.1.30.2 Receiver Query Source

```

Each line of the trace display is usually in the following format (depending on the options selected and the responses from the devices along the path):



*hop-number host (ip-address) protocolttl*

Table 150 summarizes the output fields of the display.



**NOTE:** The packet statistics gathered from Juniper Networks devices and routing nodes always display as 0.

Table 150: CLI mtrace from-source Command Output Summary

| Field                                  | Description                                                                                                                                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>hop-number</i>                      | Number of the hop (device) along the path.                                                                                                      |
| <i>host</i>                            | Hostname, if available, or IP address of the device. If the <b>no-resolve</b> option was entered in the command, the hostname is not displayed. |
| <i>ip-address</i>                      | IP address of the device.                                                                                                                       |
| <i>protocol</i>                        | Protocol used.                                                                                                                                  |
| <i>ttl</i>                             | TTL threshold.                                                                                                                                  |
| Round trip time <i>milliseconds ms</i> | Total time between the sending of the query packet and the receiving of the response packet.                                                    |
| total ttl of <i>number</i> required    | Total number of hops required to reach the source.                                                                                              |
| Source                                 | Source IP address of the response packet.                                                                                                       |
| Response Dest                          | Response destination IP address.                                                                                                                |
| Overall                                | Average packet rate for all traffic at each hop.                                                                                                |
| Packet Statistics For Traffic From     | Number of packets lost, number of packets sent, percentage of packets lost, and average packet rate at each hop.                                |
| Receiver                               | IP address receiving the multicast packets.                                                                                                     |
| Query Source                           | IP address of the host sending the query packets.                                                                                               |

Related Documentation • [Monitoring Overview on page 1397](#)



# Monitoring Application Layer Gateways Features

- [Monitoring H.323 ALG Information on page 1763](#)
- [Monitoring MGCP ALGs on page 1764](#)
- [Monitoring SCCP ALGs on page 1767](#)
- [Monitoring SIP ALGs on page 1769](#)
- [Monitoring Voice ALG H.323 on page 1774](#)
- [Monitoring Voice ALG MGCP on page 1776](#)
- [Monitoring Voice ALG SCCP on page 1779](#)
- [Monitoring Voice ALG SIP on page 1782](#)
- [Monitoring Voice ALG Summary on page 1787](#)

## Monitoring H.323 ALG Information

**Purpose** View the H.323 ALG counters information.

**Action** Select **Monitor>ALGs>H323** in the J-Web user interface, or enter the **show security alg h323 counters** command.

[Table 151](#) summarizes key output fields in the H.323 counters display.

**Table 151: Summary of Key H.323 Counters Output Fields**

| Field                             | Values                                                                                                                           | Additional Information |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>H.323 Counters Information</b> |                                                                                                                                  |                        |
| Packets received                  | Number of H.323 ALG packets received.                                                                                            | —                      |
| Packets dropped                   | Number of H.323 ALG packets dropped.                                                                                             | —                      |
| RAS message received              | Number of incoming RAS (Endpoint Registration, Admission, and Status) messages per second per gatekeeper received and processed. | —                      |

Table 151: Summary of Key H.323 Counters Output Fields (*continued*)

| Field                       | Values                                              | Additional Information                                                                                                                                                                                                            |
|-----------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Q.931 message received      | Counter for Q.931 message received.                 | —                                                                                                                                                                                                                                 |
| H.245 message received      | Counter for H.245 message received.                 | —                                                                                                                                                                                                                                 |
| Number of calls             | Total number of H.323 ALG calls.                    | —                                                                                                                                                                                                                                 |
| Number of active calls      | Number of active H.323 ALG calls.                   | This counter displays the number of call legs and might not display the exact number of voice calls that are active. For instance, for a single active voice call between two endpoints, this counter might display a value of 2. |
| <b>H.323 Error Counters</b> |                                                     |                                                                                                                                                                                                                                   |
| Decoding errors             | Number of decoding errors.                          | —                                                                                                                                                                                                                                 |
| Message flood dropped       | Error counter for message flood dropped.            | —                                                                                                                                                                                                                                 |
| NAT errors                  | H.323 ALG Network Address Translation (NAT) errors. | —                                                                                                                                                                                                                                 |
| Resource manager errors     | H.323 ALG resource manager errors.                  | —                                                                                                                                                                                                                                 |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring MGCP ALGs

This section contains the following topics:

- [Monitoring MGCP ALG Calls on page 1764](#)
- [Monitoring MGCP ALG Counters on page 1765](#)
- [Monitoring MGCP ALG Endpoints on page 1766](#)

### Monitoring MGCP ALG Calls

**Purpose** View information about MGCP ALG calls.

**Action** Select **Monitor>ALGs>MGCP>Calls** in the J-Web user interface. To view detailed information, select the endpoint on the MGCP calls page.

Alternatively, enter the **show security alg mgcp calls** command.

Table 152 summarizes key output fields in the MGCP calls display.

**Table 152: Summary of Key MGCP Calls Output Fields**

| Field                          | Values                                                                                                           | Additional Information |
|--------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>MGCP Calls Information</b>  |                                                                                                                  |                        |
| Endpoint@GW                    | Endpoint name.                                                                                                   | —                      |
| Zone                           | <ul style="list-style-type: none"> <li><b>trust</b>—Trust zone.</li> <li><b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| Call ID                        | Call identifier for ALG MGCP.                                                                                    | —                      |
| RM Group                       | Resource manager group ID.                                                                                       | —                      |
| Call Duration                  | Duration for which connection is active.                                                                         | —                      |
| Connection Id                  | Connection identifier for MGCP ALG calls.                                                                        | —                      |
| <b>Calls Details: Endpoint</b> |                                                                                                                  |                        |
| Local SDP                      | IP address of the MGCP ALG local call owner, as per the Session Description Protocol (SDP).                      | —                      |
| Remote SDP                     | Remote IP address of the MGCP ALG remote call owner, as per the Session Description Protocol (SDP).              | —                      |

## Monitoring MGCP ALG Counters

**Purpose** View MGCP ALG counters information.

**Action** Select **Monitor>ALGs>MGCP>Counters** in the J-Web user interface, or enter the **show security alg mgcp counters** command.

Table 153 summarizes key output fields in the MGCP counters display.

**Table 153: Summary of Key MGCP Counters Output Fields**

| Field                            | Values                               | Additional Information |
|----------------------------------|--------------------------------------|------------------------|
| <b>MGCP Counters Information</b> |                                      |                        |
| Packets received                 | Number of MGCP ALG packets received. | —                      |
| Packets dropped                  | Number of MGCP ALG packets dropped.  | —                      |

Table 153: Summary of Key MGCP Counters Output Fields (*continued*)

| Field                         | Values                                             | Additional Information |
|-------------------------------|----------------------------------------------------|------------------------|
| Message received              | Number of MGCP ALG messages received.              | —                      |
| Number of connections         | Number of MGCP ALG connections.                    | —                      |
| Number of active connections  | Number of active MGCP ALG connections.             | —                      |
| Number of calls               | Number of MGCP ALG calls.                          | —                      |
| Number of active calls        | Number of MGCP ALG active calls.                   | —                      |
| Number of active transactions | Number of active transactions.                     | —                      |
| Number of re-transmission     | Number of MGCP ALG retransmissions.                | —                      |
| <b>Error Counters</b>         |                                                    |                        |
| Unknown-method                | MGCP ALG unknown method errors.                    | —                      |
| Decoding error                | MGCP ALG decoding errors.                          | —                      |
| Transaction error             | MGCP ALG transaction errors.                       | —                      |
| Call error                    | MGCP ALG counter errors.                           | —                      |
| Connection error              | MGCP ALG connection errors.                        | —                      |
| Connection flood drop         | MGCP ALG connection flood drop errors.             | —                      |
| Message flood drop            | MGCP ALG message flood drop errors.                | —                      |
| IP resolve error              | MGCP ALG IP address resolution errors.             | —                      |
| NAT error                     | MGCP ALG Network Address Translation (NAT) errors. | —                      |
| Resource manager error        | MGCP ALG resource manager errors.                  | —                      |

## Monitoring MGCP ALG Endpoints

**Purpose** View information about MGCP ALG endpoints.

**Action** Select **Monitor>ALGs>MGCP>Endpoints** in the J-Web user interface. To view detailed information, select the gateway on the MGCP endpoints page.

Alternatively, enter the **show security alg mgcp endpoints** command.

Table 154 summarizes key output fields in the MGCP endpoints display.

**Table 154: Summary of Key MGCP Endpoints Output Fields**

| Field                          | Values                                                                                                           | Additional Information |
|--------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>MGCP Endpoints</b>          |                                                                                                                  |                        |
| Gateway                        | IP address of the gateway.                                                                                       | —                      |
| Zone                           | <ul style="list-style-type: none"> <li><b>trust</b>—Trust zone.</li> <li><b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| IP                             | IP address.                                                                                                      | —                      |
| <b>Endpoints: Gateway name</b> |                                                                                                                  |                        |
| Endpoint                       | Endpoint name.                                                                                                   | —                      |
| Transaction #                  | Transaction identifier.                                                                                          | —                      |
| Call #                         | Call identifier.                                                                                                 | —                      |
| Notified Entity                | The certificate authority (CA) currently controlling the gateway.                                                | —                      |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring SCCP ALGs

This section contains the following topics:

- [Monitoring SCCP ALG Calls on page 1767](#)
- [Monitoring SCCP ALG Counters on page 1768](#)

### Monitoring SCCP ALG Calls

**Purpose** View information about SCCP ALG calls.

**Action** Select **Monitor>ALGs>SCCP>Calls** in the J-Web user interface. To view detailed information, select the client IP address on the SCCP calls page.

Alternatively, enter the **show security alg sccp calls** command.

Table 155 summarizes key output fields in the SCCP calls display.

Table 155: Summary of Key SCCP Calls Output Fields

| Field                         | Values                             | Additional Information |
|-------------------------------|------------------------------------|------------------------|
| <b>SCCP Calls Information</b> |                                    |                        |
| Client IP                     | IP address of the client.          | —                      |
| Zone                          | Client zone identifier.            | —                      |
| Call Manager                  | IP address of the call manager.    | —                      |
| Conference ID                 | Conference call identifier.        | —                      |
| RM Group                      | Resource manager group identifier. | —                      |

## Monitoring SCCP ALG Counters

**Purpose** View SCCP ALG counters information.

**Action** Select **Monitor>ALGs>SCCP>Count** in the J-Web user interface, or enter the **show security alg sccp counters** command.

Table 156 summarizes key output fields in the SCCP counters display.

Table 156: Summary of Key SCCP Counters Output Fields

| Field                            | Values                                                   | Additional Information |
|----------------------------------|----------------------------------------------------------|------------------------|
| <b>SCCP Counters Information</b> |                                                          |                        |
| Clients currently registered     | Number of SCCP ALG clients currently registered.         | —                      |
| Active calls                     | Number of active SCCP ALG calls.                         | —                      |
| Total calls                      | Total number of SCCP ALG calls.                          | —                      |
| Packets received                 | Number of SCCP ALG packets received.                     | —                      |
| PDUs processed                   | Number of SCCP ALG protocol data units (PDUs) processed. | —                      |
| Current call rate                | Number of calls per second.                              | —                      |
| <b>Error counters</b>            |                                                          |                        |
| Packets dropped                  | Number of packets dropped by the SCCP ALG.               | —                      |



Table 156: Summary of Key SCCP Counters Output Fields (*continued*)

| Field                      | Values                                                                      | Additional Information |
|----------------------------|-----------------------------------------------------------------------------|------------------------|
| Decode errors              | SCCP ALG decoding errors.                                                   | —                      |
| Protocol errors            | Number of protocol errors.                                                  | —                      |
| Address translation errors | Number of Network Address Translation (NAT) errors encountered by SCCP ALG. | —                      |
| Policy lookup errors       | Number of packets dropped because of a failed policy lookup.                | —                      |
| Unknown PDUs               | Number of unknown protocol data units (PDUs).                               | —                      |
| Maximum calls exceed       | Number of times the maximum SCCP calls limit was exceeded.                  | —                      |
| Maximum call rate exceed   | Number of times the maximum SCCP call rate exceeded.                        | —                      |
| Initialization errors      | Number of initialization errors.                                            | —                      |
| Internal errors            | Number of internal errors.                                                  | —                      |
| Unsupported feature        | Number of unsupported feature errors.                                       | —                      |
| Non specific error         | Number of nonspecific errors.                                               | —                      |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring SIP ALGs

This section contains the following topics:

- [Monitoring SIP ALG Calls on page 1770](#)
- [Monitoring SIP ALG Counters on page 1770](#)

- [Monitoring SIP ALG Rate Information on page 1772](#)
- [Monitoring SIP ALG Transactions on page 1773](#)

## Monitoring SIP ALG Calls

**Purpose** View information about SIP ALG calls.

**Action** Select **Monitor>ALGs>SIP>Calls** in the J-Web user interface. To view detailed information, select the Call Leg on the SIP calls page.

Alternatively, enter the **show security alg sip calls detail** command.

[Table 157](#) summarizes key output fields in the SIP calls display.

**Table 157: Summary of Key SIP Calls Output Fields**

| Field                        | Values                                        | Additional Information |
|------------------------------|-----------------------------------------------|------------------------|
| <b>SIP Calls Information</b> |                                               |                        |
| Call Leg                     | Call length identifier.                       | —                      |
| Zone                         | Client zone identifier.                       | —                      |
| RM Group                     | Resource manager group identifier.            | —                      |
| Local Tag                    | Local tag for the SIP ALG User Agent server.  | —                      |
| Remote Tag                   | Remote tag for the SIP ALG User Agent server. | —                      |

## Monitoring SIP ALG Counters

**Purpose** View SIP ALG counters information.

**Action** Select **Monitor>ALGs>SIP>Count** in the J-Web user interface, or enter the **show security alg sip counters** command.

[Table 158](#) summarizes key output fields in the SIP counters display.

**Table 158: Summary of Key SIP Counters Output Fields**

| Field                           | Values                          | Additional Information                                                                                                                                                                                              |
|---------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Counters Information</b> |                                 |                                                                                                                                                                                                                     |
| INVITE                          | Number of INVITE requests sent. | An INVITE request is sent to invite another user to participate in a session.                                                                                                                                       |
| CANCEL                          | Number of CANCEL requests sent. | A user can send a CANCEL request to cancel a pending INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE had sent a final response for the INVITE before it received the CANCEL. |

Table 158: Summary of Key SIP Counters Output Fields (*continued*)

| Field                     | Values                             | Additional Information                                                                                                                                                                                                                                                              |
|---------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACK                       | Number of ACK requests sent.       | The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request.                                                                                                                                                     |
| BYE                       | Number of BYE requests sent.       | A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.                                                                                                                                                               |
| REGISTER                  | Number of REGISTER requests sent.  | A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. A SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user. |
| OPTIONS                   | Number of OPTIONS requests sent.   | An OPTION message is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports.                                             |
| INFO                      | Number of INFO requests sent.      | An INFO message is used to communicate mid-session signaling information along the signaling path for the call.                                                                                                                                                                     |
| MESSAGE                   | Number of MESSAGE requests sent.   | SIP messages consist of requests from a client to a server and responses to the requests from a server to a client with the purpose of establishing a session (or a call).                                                                                                          |
| NOTIFY                    | Number of NOTIFY requests sent.    | A NOTIFY message is sent to inform subscribers of changes in state to which the subscriber has a subscription.                                                                                                                                                                      |
| REFER                     | Number of REFER requests sent.     | A REFER request is used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request.                                                                                                                                 |
| SUBSCRIBE                 | Number of SUBSCRIBE requests sent. | A SUBSCRIBE request is used to request current state and state updates from a remote node.                                                                                                                                                                                          |
| UPDATE                    | Number of UPDATE requests sent.    | An UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updated Session Description Protocol (SDP) information. The following header fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route.                            |
| <b>SIP Error Counters</b> |                                    |                                                                                                                                                                                                                                                                                     |
| Total Pkt-in              | SIP ALG total packets received.    | —                                                                                                                                                                                                                                                                                   |

Table 158: Summary of Key SIP Counters Output Fields (*continued*)

| Field                       | Values                                                                            | Additional Information |
|-----------------------------|-----------------------------------------------------------------------------------|------------------------|
| Total Pkt dropped on error  | Number of packets dropped by the SIP ALG.                                         | —                      |
| Transaction error           | SIP ALG transaction errors.                                                       | —                      |
| Call error                  | SIP ALG call errors.                                                              | —                      |
| IP resolve error            | SIP ALG IP address resolution errors.                                             | —                      |
| NAT error                   | SIP ALG NAT errors.                                                               | —                      |
| Resource manager error      | SIP ALG resource manager errors.                                                  | —                      |
| RR header exceeded max      | Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit. | —                      |
| Contact header exceeded max | Number of times the SIP ALG contact header exceeded the maximum limit.            | —                      |
| Call dropped due to limit   | SIP ALG calls dropped because of call limits.                                     | —                      |
| SIP stack error             | SIP ALG stack errors.                                                             | —                      |

## Monitoring SIP ALG Rate Information

**Purpose** View SIP ALG rate information.

**Action** Select **Monitor>ALGs>SIP>Rate** in the J-Web user interface, or enter the **show security alg sip rate** command.

Table 159 summarizes key output fields in the SIP rate display.

Table 159: Summary of Key SIP Rate Output Fields

| Field                | Values | Additional Information |
|----------------------|--------|------------------------|
| SIP Rate Information |        |                        |

Table 159: Summary of Key SIP Rate Output Fields (*continued*)

| Field                                              | Values                                                                                                                                       | Additional Information |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| CPU ticks per microseconds is                      | SIP ALG CPU ticks per microsecond.                                                                                                           | –                      |
| Time taken for the last message in microseconds is | Time, in microseconds, that the last SIP ALG message needed to transit the network.                                                          | –                      |
| Number of messages in 10 minutes                   | Total number of SIP ALG messages transiting the network in 10 minutes.                                                                       | –                      |
| Time taken by the messages in 10 minutes           | Total time, in microseconds, during an interval of less than 10 minutes for the specified number of SIP ALG messages to transit the network. | –                      |
| Rate                                               | Number of SIP ALG messages per second transiting the network.                                                                                | –                      |

## Monitoring SIP ALG Transactions

**Purpose** View information about SIP ALG transactions.

**Action** Select **Monitor>ALGs>SIP>Transactions** in the J-Web user interface, or enter the **show security alg sip transactions** command.

Table 160 summarizes key output fields in the SIP transactions display.

Table 160: Summary of Key SIP Transactions Output Fields

| Field                               | Values                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Information |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>SIP Transactions Information</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                   |                        |
| Transaction Name                    | <ul style="list-style-type: none"> <li>• <b>UAS</b>—SIP ALG User Agent server transaction name.</li> <li>• <b>UAC</b>—SIP ALG User Agent client transaction name.</li> </ul>                                                                                                                                                                                                                                                      | –                      |
| Method                              | <p>The method to be performed on the resource. Possible methods:</p> <ul style="list-style-type: none"> <li>• <b>INVITE</b>—Initiate call</li> <li>• <b>ACK</b>—Confirm final response</li> <li>• <b>BYE</b>—Terminate and transfer call</li> <li>• <b>CANCEL</b>—Cancel searches and “ringing”</li> <li>• <b>OPTIONS</b>—Features support by the other side</li> <li>• <b>REGISTER</b>—Register with location service</li> </ul> | –                      |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring Voice ALG H.323

**Purpose** Use the monitoring functionality to view the ALG H.323 page.

**Action** To monitor ALG H.323 select **Monitor>Security>Voice ALGs>H.323** in the J-Web user interface.

**Meaning** [Table 161](#) summarizes key output fields in the ALG H.323 page.

**Table 161: ALG H.323 Monitoring Page**

| Field                     | Value                                            | Additional Information                            |
|---------------------------|--------------------------------------------------|---------------------------------------------------|
| Virtual Chassis Member    | Display the list of virtual chassis member.      | Select one of the virtual chassis members listed. |
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. | Select the time interval from the drop-down list. |
| Refresh                   | Displays the option to refresh the page.         | —                                                 |
| Clear                     | Provides an option to clear the monitor summary. | Click <b>clear</b> to clear the monitor summary.  |

### H.323 Counter Summary

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |   |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Category | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Packets received</b>—Number of ALG H.323 packets received.</li> <li>• <b>Packets dropped</b>—Number of ALG H.323 packets dropped.</li> <li>• <b>RAS message received</b> Number of incoming RAS (Registration, Admission, and Status) messages per second per gatekeeper received and processed.</li> <li>• <b>Q.931 message received</b>—Counter for Q.931 message received.</li> <li>• <b>H.245 message received</b>— Counter for H.245 message received.</li> <li>• <b>Number of calls</b>—Total number of ALG H.323 calls.</li> <li>• <b>Number of active calls</b>—Number of active ALG H.323 calls.</li> <li>• <b>Number of DSCP Marked</b>—Number of DSCP Marked on ALG H.323 calls.</li> </ul> | — |
| Count    | Provides count of response codes for each H.323 counter summary category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | — |

### H.323 Error Counter

Table 161: ALG H.323 Monitoring Page (*continued*)

| Field                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Additional Information |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Category                     | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Decoding errors</b>—Number of decoding errors.</li> <li>• <b>Message flood dropped</b>—Error counter for message flood dropped.</li> <li>• <b>NAT errors</b>—H.323 ALG NAT errors.</li> <li>• <b>Resource manager errors</b>—H.323 ALG resource manager errors.</li> <li>• <b>DSCP Marked errors</b>—H.323 ALG DSCP marked errors.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | —                      |
| Count                        | Provides count of response codes for each H.323 error counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —                      |
| <b>Counter Summary Chart</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                        |
| Packets Received             | Provides the graphical representation of the packets received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | —                      |
| <b>H.323 Message Counter</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                        |
| Category                     | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>RRQ</b>—Registration Request message counter.</li> <li>• <b>RCF</b>—Registration Confirmation Message.</li> <li>• <b>ARQ</b>—Admission Request message counter.</li> <li>• <b>ACF</b>—Admission Confirmation</li> <li>• <b>URQ</b>—Unregistration Request.</li> <li>• <b>UCF</b>—Unregistration Confirmation.</li> <li>• <b>DRQ</b>—Disengage Request.</li> <li>• <b>DCF</b>—Disengage Confirmation.</li> <li>• <b>Oth RAS</b>—Other incoming Registration, Admission, and Status messages message counter.</li> <li>• <b>Setup</b>—Timeout value, in seconds, for the response of the outgoing setup message.</li> <li>• <b>Alert</b>—Alert message type.</li> <li>• <b>Connect</b>—Connect setup process.</li> <li>• <b>CallProd</b>—Number of call production messages sent.</li> <li>• <b>Info</b>—Number of info requests sent.</li> <li>• <b>RelCmpl</b>—Number of Rel Cmpl message ssent.</li> <li>• <b>Facility</b>—Number of facility messages sent.</li> <li>• <b>Empty</b>—Empty capabilities to the support message counter.</li> <li>• <b>OLC</b>—Open Local Channel message counter.</li> <li>• <b>OLC ACK</b>—Open Local Channel Acknowledge message counter.</li> <li>• <b>Oth H245</b>—Other H.245 message counter</li> </ul> | —                      |
| Count                        | Provides count of response codes for each H.323 message counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |

- Related Documentation**
- [Monitoring Voice ALG Summary on page 1787](#)
  - [Monitoring Voice ALG MGCP on page 1776](#)
  - [Monitoring Voice ALG SCCP on page 1779](#)
  - [Monitoring Voice ALG SIP on page 1782](#)

## Monitoring Voice ALG MGCP

**Purpose** Use the monitoring functionality to view the voice ALG MGCP page.

**Action** To monitor ALG MGCP, select **Monitor>Security>Voice ALGs>MGCP** in the J-Web user interface.

**Meaning** [Table 162](#) summarizes key output fields in the voice ALG MGCP page.

**Table 162: Voice ALG MGCP Monitoring Page**

| Field                        | Value                                            | Additional Information                            |
|------------------------------|--------------------------------------------------|---------------------------------------------------|
| Virtual Chassis Member       | Displays the list of virtual chassis member.     | Select one of the virtual chassis members listed. |
| Refresh Interval (30 sec)    | Displays the time interval set for page refresh. | Select the time interval from the drop-down list. |
| Refresh                      | Displays the option to refresh the page.         | —                                                 |
| Clear                        | Provides an option to clear the monitor summary. | Click <b>Clear</b> to clear the monitor summary.  |
| <b>Counters</b>              |                                                  |                                                   |
| <b>MGCP Counters Summary</b> |                                                  |                                                   |



Table 162: Voice ALG MGCP Monitoring Page (*continued*)

| Field    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Additional Information |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Category | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Packets Received</b>—Number of ALG MGCP packets received.</li> <li>• <b>Packets Dropped</b>— Number of ALG MGCP packets dropped.</li> <li>• <b>Message received</b>— Number of ALG MGCP messages received.</li> <li>• <b>Number of connections</b>— Number of ALG MGCP connections.</li> <li>• <b>Number of active connections</b>— Number of active ALG MGCP connections.</li> <li>• <b>Number of calls</b>— Number of ALG MGCP calls.</li> <li>• <b>Number of active calls</b>— Number of active ALG MGCP calls.</li> <li>• <b>Number of active transactions</b>— Number of active transactions.</li> <li>• <b>Number of transactions</b>— Number of transactions.</li> <li>• <b>Number of re-transmission</b>—Number of ALG MGCP retransmissions.</li> <li>• <b>Number of active endpoints</b>— Number of MGCP active endpoints.</li> <li>• <b>Number of DSCP marked</b>— Number of MGCP DSCPs marked.</li> </ul> | —                      |
| Count    | Provides the count of response codes for each MGCP counter summary category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                      |

#### MGCP Error Counter

Table 162: Voice ALG MGCP Monitoring Page (*continued*)

| Field                       | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Additional Information |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Category                    | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Unknown-method</b>— MGCP ALG unknown method errors.</li> <li>• <b>Decoding error</b>— MGCP ALG decoding errors.</li> <li>• <b>Transaction error</b>— MGCP ALG transaction errors.</li> <li>• <b>Call error</b>— MGCP ALG call ounter errors.</li> <li>• <b>Connection error</b>— MGCP ALG connection errors.</li> <li>• <b>Connection flood drop</b>— MGCP ALG connection flood drop errors.</li> <li>• <b>Message flood drop</b>— MGCP ALG message flood drop error.</li> <li>• <b>IP resolve error</b>— MGCP ALG IP address resolution errors.</li> <li>• <b>NAT error</b>— MGCP ALG NAT errors.</li> <li>• <b>Resource manager error</b>— MGCP ALG resource manager errors.</li> <li>• <b>DSCP Marked error</b>— MGCP ALG DSCP marked errors.</li> </ul> | —                      |
| Count                       | Provides the count of response codes for each summary error counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | —                      |
| Counter Summary Chart       | Displays the Counter Summary Chart.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                      |
| <b>MGCP Packet Counters</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                        |
| Category                    | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>CRCX</b>— Create Connection</li> <li>• <b>MDCX</b>— Modify Connection</li> <li>• <b>DLCX</b>— Delete Connection</li> <li>• <b>AUEP</b>— Audit Endpoint</li> <li>• <b>AUCX</b>— Audit Connection</li> <li>• <b>NTFY</b>— Notify MGCP</li> <li>• <b>RSIP</b>— Restart in Progress</li> <li>• <b>EPCF</b>— Endpoint Configuration</li> <li>• <b>RQNT</b>— Request for Notification</li> <li>• <b>000-199</b>—Respond code is 0-199</li> <li>• <b>200-299</b>—Respond code is 200-299</li> <li>• <b>300-399</b>—Respond code is 300-399</li> </ul>                                                                                                                                                                                                              | —                      |
| Count                       | Provides count of response codes for each MGCP packet counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | —                      |
| <b>Calls</b>                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                        |

Table 162: Voice ALG MGCP Monitoring Page (*continued*)

| Field         | Value                                                                                                                                                | Additional Information |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Endpoint@GW   | Displays the endpoint name.                                                                                                                          | —                      |
| Zone          | Displays the following options: <ul style="list-style-type: none"> <li>• <b>trust</b>—Trust zone.</li> <li>• <b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| Endpoint IP   | Displays the endpoint IP address.                                                                                                                    | —                      |
| Call ID       | Displays the call identifier for ALG MGCP.                                                                                                           | —                      |
| RM Group      | Displays the resource manager group ID.                                                                                                              | —                      |
| Call Duration | Displays the duration for which connection is active.                                                                                                | —                      |

- Related Documentation**
- [Monitoring Voice ALG Summary on page 1787](#)
  - [Monitoring Voice ALG H.323 on page 1774](#)
  - [Monitoring Voice ALG SCCP on page 1779](#)
  - [Monitoring Voice ALG SIP on page 1782](#)

## Monitoring Voice ALG SCCP

**Purpose** Use the monitoring functionality to view the voice ALG SCCP page.

**Action** To monitor voice ALG SCCP, select **Monitor>Security>Voice ALGs>SCCP** in the J-Web user interface.

**Meaning** [Table 163](#) summarizes key output fields in the voice ALG SCCP page.

Table 163: Voice ALG SCCP Monitoring Page

| Field                     | Value                                            | Additional Information                            |
|---------------------------|--------------------------------------------------|---------------------------------------------------|
| Virtual Chassis Member    | Displays the list of virtual chassis member.     | Select one of the virtual chassis members listed. |
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. | Select the time interval from the drop-down list. |
| Refresh                   | Displays the option to refresh the page.         | —                                                 |
| Clear                     | Provides an option to clear the monitor summary. | Click <b>Clear</b> to clear the monitor summary.  |

Table 163: Voice ALG SCCP Monitoring Page (*continued*)

| Field                       | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Additional Information |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>SCCP Call Statistics</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                        |
| Category                    | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Active client sessions</b>— Number of active SCCP ALG client sessions.</li> <li>• <b>Active calls</b>— Number of active SCCP ALG calls.</li> <li>• <b>Total calls</b>— Total number of SCCP ALG calls.</li> <li>• <b>Packets received</b>— Number of SCCP ALG packets received.</li> <li>• <b>PDUs processed</b>— Number of SCCP ALG protocol data units (PDUs) processed.</li> <li>• <b>Current call rate</b>— Number of calls per second.</li> <li>• <b>DSCPs Marked</b>— Number of DSCP marked.</li> </ul> | —                      |
| Count                       | Provides count of response codes for each SCCP call statistics category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |
| Call Statistics Chart       | Displays the Call Statistics chart.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | —                      |
| <b>SCCP Error Counters</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                        |

Table 163: Voice ALG SCCP Monitoring Page (*continued*)

| Field         | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Additional Information |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Category      | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Packets dropped</b>— Number of packets dropped by the SCCP ALG.</li> <li>• <b>Decode errors</b>— Number of SCCP ALG decoding errors.</li> <li>• <b>Protocol errors</b>— Number of protocol errors.</li> <li>• <b>Address translation errors</b>— Number of NAT errors encountered by SCCP ALG.</li> <li>• <b>Policy lookup errors</b>— Number of packets dropped because of a failed policy lookup.</li> <li>• <b>Unknown PDUs</b>— Number of unknown PDUs.</li> <li>• <b>Maximum calls exceed</b>— Number of times the maximum SCCP calls limit was exceeded.</li> <li>• <b>Maximum call rate exceed</b>— Number of times the maximum SCCP call rate was exceeded.</li> <li>• <b>Initialization errors</b>— Number of initialization errors.</li> <li>• <b>Internal errors</b>— Number of internal errors.</li> <li>• <b>Nonspecific errors</b>— Number of nonspecific errors.</li> <li>• <b>No active calls to be deleted</b>— Number of no active calls to be deleted.</li> <li>• <b>No active client sessions to be deleted</b>— Number of no active client sessions to be deleted.</li> <li>• <b>Session cookie created error</b>— Number of session cookie created errors.</li> <li>• <b>Invalid NAT cookies deleted</b>— Number of invalid NAT cookies deleted.</li> <li>• <b>NAT cookies not found</b>— Number of NAT cookies not found.</li> <li>• <b>DSCP Marked Error</b>— Number of DSCP marked errors.</li> </ul> | —                      |
| Count         | Provides count of response codes for each SCCP error counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                      |
| <b>Calls</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                        |
| Client IP     | Displays the IP address of the client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                      |
| Zone          | Displays the client zone identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | —                      |
| Call Manager  | Displays the IP address of the call manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | —                      |
| Conference ID | Displays the conference call identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —                      |
| RM Group      | Displays the resource manager group identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | —                      |

**Related Documentation** • [Monitoring Voice ALG Summary on page 1787](#)

- [Monitoring Voice ALG H.323 on page 1774](#)
- [Monitoring Voice ALG MGCP on page 1776](#)
- [Monitoring Voice ALG SIP on page 1782](#)

## Monitoring Voice ALG SIP

**Purpose** Use the monitoring functionality to view the voice ALG SIP page.

**Action** To monitor voice ALG SIP select **Monitor>Security>Voice ALGs>SIP** in the J-Web user interface.

**Meaning** [Table 164](#) summarizes key output fields in the voice ALG SIP page.

**Table 164: Voice ALG SIP Monitoring Page**

| Field                     | Value                                            | Additional Information                            |
|---------------------------|--------------------------------------------------|---------------------------------------------------|
| Virtual Chassis Member    | Displays the list of virtual chassis members.    | Select one of the virtual chassis members listed. |
| Refresh Interval (30 sec) | Displays the time interval set for page refresh. | Select the time interval from the drop-down list. |
| Refresh                   | Displays the option to refresh the page.         | –                                                 |
| Clear                     | Provides an option to clear the monitor summary. | Click <b>Clear</b> to clear the monitor summary.  |

### Counters

#### SIP Counters Information

Table 164: Voice ALG SIP Monitoring Page (continued)

| Field  | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Additional Information |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Method | <p>Displays the SIP counter information. The available options are:</p> <ul style="list-style-type: none"><li>• <b>BYE</b>— Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.</li><li>• <b>REGISTER</b>— Number of REGISTER requests sent. A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. The SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user.</li><li>• <b>OPTIONS</b>— Number of OPTIONS requests sent. An OPTION message is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports.</li><li>• <b>INFO</b>— Number of INFO requests sent. An INFO message is used to communicate mid-session signaling information along the signaling path for the call.</li><li>• <b>MESSAGE</b>— Number of MESSAGE requests sent. SIP messages consist of requests from a client to the server and responses to the requests from the server to a client for the purpose of establishing a session (or a call).</li></ul> | —                      |

SIP Counters Information (continued)

Table 164: Voice ALG SIP Monitoring Page (*continued*)

| Field        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Additional Information |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Method       | <ul style="list-style-type: none"> <li>• <b>NOTIFY</b>— Number of NOTIFY requests sent. A NOTIFY message is sent to inform subscribers about the change in state of the subscription.</li> <li>• <b>PRACK</b>— Number of PRACK requests sent. The PRACK request plays the same role as the ACK request, but for provisional responses.</li> <li>• <b>PUBLISH</b>— Number of PUBLISH requests sent. The PUBLISH request is used for publishing the event state. PUBLISH is similar to REGISTER that allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user.</li> <li>• <b>REFER</b>— Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party identified by the contact information provided in the request.</li> <li>• <b>SUBSCRIBE</b>— Number of SUBSCRIBE requests sent. A SUBSCRIBE request is used to request current state and state information updates from a remote node.</li> <li>• <b>UPDATE</b>— Number of UPDATE requests sent. An UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updated Session Description Protocol (SDP) information. The following header fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route.</li> <li>• <b>BENOTIFY</b>— Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY.</li> <li>• <b>SERVICE</b>— Number of SERVICE requests sent. The SERVICE method is used by a SIP client to request a service from a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user that is performing the service.</li> <li>• <b>OTHER</b>— Number of OTHER requests sent.</li> </ul> | —                      |
| T, RT        | Displays the transmit and retransmit method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —                      |
| 1xx, RT      | Displays one transmit and retransmit method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —                      |
| 2xx, RT      | Displays two transmit and retransmit methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |
| 3xx, RT      | Displays three transmit and retransmit methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | —                      |
| 4xx, RT      | Displays four transmit and retransmit methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | —                      |
| 5xx, RT      | Displays five transmit and retransmit methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | —                      |
| 6xx, RT      | Displays six transmit and retransmit methods.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |
| <b>Calls</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                        |
| Call ID      | Displays the call ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | —                      |



Table 164: Voice ALG SIP Monitoring Page *(continued)*

| Field               | Value                                                                                                                                                                                                                           | Additional Information |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Method              | Displays the call method used.                                                                                                                                                                                                  | –                      |
| State               | Displays the state of the ALG SIP.                                                                                                                                                                                              | –                      |
| Group ID            | Displays the group identifier.                                                                                                                                                                                                  | –                      |
| Invite Method Chart | Displays the invite method chart. The available options are: <ul style="list-style-type: none"><li>• T/RT</li><li>• 1xx/ RT</li><li>• 2xx/ RT</li><li>• 3xx/ RT</li><li>• 4xx/ RT</li><li>• 5xx/ RT</li><li>• 6xx/ RT</li></ul> | –                      |

SIP Error Counters

Table 164: Voice ALG SIP Monitoring Page (*continued*)

| Field    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Additional Information |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Category | <p>Displays the SIP error counters. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Total Pkt-in</b>— Number of SIP ALG total packets received.</li> <li>• <b>Total Pkt dropped on error</b>— Number of packets dropped by the SIP ALG.</li> <li>• <b>Call error</b>— SIP Number of ALG call errors.</li> <li>• <b>IP resolve error</b>— Number of SIP ALG IP address resolution errors.</li> <li>• <b>NAT error</b>— SIP Number of ALG NAT errors.</li> <li>• <b>Resource manager error</b>— Number of SIP ALG resource manager errors.</li> <li>• <b>RR header exceeded max</b>— Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit.</li> <li>• <b>Contact header exceeded max</b>— Number of times the SIP ALG contact header exceeded the maximum limit.</li> <li>• <b>Call dropped due to limit</b>— Number of SIP ALG calls dropped because of call limits.</li> <li>• <b>SIP stack error</b>— Number of SIP ALG stack errors.</li> <li>• <b>SIP Decode error</b>— Number of SIP ALG decode errors.</li> <li>• <b>SIP unknown method error</b>— Number of SIP ALG unknow method errors.</li> <li>• <b>SIP DSCP marked</b>—SIP ALG DSCP marked.</li> <li>• <b>SIP DSCP marked error</b>— Number of SIP ALG DSCPs marked.</li> <li>• <b>RTO message sent</b>— Number of SIP ALG marked RTO messages sent.</li> <li>• <b>RTO message received</b>— Number of SIP ALG RTO messages received.</li> <li>• <b>RTO buffer allocation failure</b>— Number of SIP ALG RTO buffer allocation failures.</li> <li>• <b>RTO buffer transmit failure</b>— Number of SIP ALG RTO buffer transmit failures.</li> <li>• <b>RTO send processing error</b>— Number of SIP ALG RTO send processing errors.</li> <li>• <b>RTO receiving processing error</b>— Number of SIP ALG RTO receiving processing errors.</li> <li>• <b>RTO receive invalid length</b>— Number of SIP ALG RTOs receiving invalid length.</li> <li>• <b>RTO receive call process error</b>— Number of SIP ALG RTO receiving call process errors.</li> <li>• <b>RTO receive call allocation error</b>— Number of SIP ALG RTO receiving call allocation error.</li> <li>• <b>RTO receive call register error</b>— Number of SIP ALG RTO receiving call register errors.</li> <li>• <b>RTO receive invalid status error</b>— Number of SIP ALG RTO receiving register errors.</li> </ul> | —                      |
| Count    | Provides count of response codes for each SIP ALG counter category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | —                      |

- Related Documentation**
- [Monitoring Voice ALG Summary on page 1787](#)
  - [Monitoring Voice ALG H.323 on page 1774](#)
  - [Monitoring Voice ALG MGCP on page 1776](#)
  - [Monitoring Voice ALG SCCP on page 1779](#)

## Monitoring Voice ALG Summary

**Purpose** Use the monitoring functionality to view the voice ALG summary page.

**Action** To monitor voice ALG summary, select **Monitor>Security>Voice ALGs>Summary** in the J-Web user interface.

**Meaning** [Table 165](#) summarizes key output fields in the voice ALG summary page.

**Table 165: Voice ALG Summary Monitoring Page**

| Field                      | Value                                            | Additional Information                            |
|----------------------------|--------------------------------------------------|---------------------------------------------------|
| Virtual Chassis Member     | Display the list of virtual chassis member.      | Select one of the virtual chassis members listed. |
| Refresh Interval (30 sec)  | Displays the time interval set for page refresh. | Select the time interval from the drop-down list. |
| Refresh                    | Displays the option to refresh the page.         | –                                                 |
| Clear                      | Provides an option to clear the monitor summary. | Click <b>Clear</b> to clear the monitor summary.  |
| Protocol Name              | Displays the protocols configured.               | –                                                 |
| Total Calls                | Displays the total number of calls.              | –                                                 |
| Number of Active Calls     | Displays the number of active calls.             | –                                                 |
| Number of Received Packets | Displays the number of packets received.         | –                                                 |
| Number of Errors           | Displays the number of errors.                   | –                                                 |
| H.323 Calls Chart          | Displays the H.323 calls chart.                  | –                                                 |
| MGCP Calls Chart           | Displays the MGCP calls chart.                   | –                                                 |
| SCCP Calls Chart           | Displays the SCCP calls chart.                   | –                                                 |
| SIP Calls Chart            | Displays the SIP calls chart.                    | –                                                 |

- Related Documentation**
- [Monitoring Voice ALG H.323 on page 1774](#)
  - [Monitoring Voice ALG MGCP on page 1776](#)
  - [Monitoring Voice ALG SCCP on page 1779](#)
  - [Monitoring Voice ALG SIP on page 1782](#)

# Monitoring Interfaces and Switching Functions

- [Displaying Real-Time Interface Information on page 1789](#)
- [Monitoring Address Pools on page 1791](#)
- [Monitoring Ethernet Switching on page 1792](#)
- [Monitoring GVRP on page 1793](#)
- [Monitoring Interfaces on page 1794](#)
- [Monitoring MPLS Traffic Engineering Information on page 1795](#)
- [Monitoring PPP on page 1800](#)
- [Monitoring PPPoE on page 1801](#)
- [Monitoring Spanning Tree on page 1805](#)
- [Monitoring the WAN Acceleration Interface on page 1806](#)

## Displaying Real-Time Interface Information

---

Enter the **monitor interface** command to display real-time traffic, error, alarm, and filter statistics about a physical or logical interface:

```
user@host> monitor interface (interface-name | traffic)
```

Replace ***interface-name*** with the name of a physical or logical interface. If you specify the **traffic** option, statistics for all active interfaces display.

The real-time statistics update every second. The **Current delta** and **Delta** columns display the amount the statistics counters have changed since the **monitor interface** command was entered or since you cleared the delta counters. [Table 166](#) and [Table 167](#) list the keys you use to control the display using the ***interface-name*** and **traffic** options. (The keys are not case sensitive.)

**Table 166: CLI monitor interface Output Control Keys**

| Key | Action                                                                                                                |
|-----|-----------------------------------------------------------------------------------------------------------------------|
| c   | Clears (returns to 0) the delta counters in the <b>Current delta</b> column. The statistics counters are not cleared. |

Table 166: CLI monitor interface Output Control Keys (*continued*)

| Key      | Action                                                                                                                                                                                                   |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| f        | Freezes the display, halting the update of the statistics and delta counters.                                                                                                                            |
| i        | Displays information about a different interface. You are prompted for the name of a specific interface.                                                                                                 |
| n        | Displays information about the next interface. The device scrolls through the physical and logical interfaces in the same order in which they are displayed by the <b>show interfaces terse</b> command. |
| q or ESC | Quits the command and returns to the command prompt.                                                                                                                                                     |
| t        | Thaws the display, resuming the update of the statistics and delta counters.                                                                                                                             |

Table 167: CLI monitor interface traffic Output Control Keys

| Key      | Action                                                                                                        |
|----------|---------------------------------------------------------------------------------------------------------------|
| b        | Displays the statistics in units of bytes and bytes per second (bps).                                         |
| c        | Clears (returns to 0) the delta counters in the <b>Delta</b> column. The statistics counters are not cleared. |
| d        | Displays the <b>Delta</b> column instead of the rate column—in bps or packets per second (pps).               |
| p        | Displays the statistics in units of packets and packets per second (pps).                                     |
| q or ESC | Quits the command and returns to the command prompt.                                                          |
| r        | Displays the rate column—in bps and pps—instead of the <b>Delta</b> column.                                   |

The following are sample displays from the **monitor interface** command:

```
user@host> monitor interface fe-0/0/0
```

```

host1 Seconds: 5 Time: 04:38:40
 Delay: 3/0/10

Interface: fe-0/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 1000mbps
Traffic statistics: Current delta
 Input bytes: 885405423 (3248 bps) [2631]
 Output bytes: 137411893 (3344 bps) [10243]
 Input packets: 7155064 (2 pps) [28]
 Output packets: 636071 (1 pps) [23]
Error statistics:
 Input errors: 0 [0]
 Input drops: 0 [0]
 Input framing errors: 0 [0]
 Policed discards: 0 [0]
 L3 incompletes: 0 [0]
```

```

L2 channel errors: 0 [0]
L2 mismatch timeouts: 0 [0]
Carrier transitions: 1 [0]
Output errors: 0 [0]
Output drops: 0 [0]
Aged packets: 0 [0]
Active alarms : None
Active defects: None
Input MAC/Filter statistics:
 Unicast packets 73083 [16]
 Broadcast packets 3629058 [5]
 Multicast packets 3511364 [3]
 Oversized frames 0 [0]
 Packet reject count 0 [0]
 DA rejects 0 [0]
 SA rejects 0 [0]
Output MAC/Filter Statistics:
 Unicast packets 629555 [28]
 Broadcast packets 6494 Multicast packet [0]

```



**NOTE:** The output fields that display when you enter the **monitor interface** *interface-name* command are determined by the interface you specify.

```
user@host> monitor interface traffic
```

| Interface | Link | Input packets | (pps)   | Output packets | (pps)   |
|-----------|------|---------------|---------|----------------|---------|
| fe-0/0/0  | Up   | 42334         | (5)     | 23306          | (3)     |
| fe-0/0/1  | Up   | 587525876     | (12252) | 589621478      | (12891) |

**Related Documentation** • [Monitoring Interfaces on page 1794](#)

## Monitoring Address Pools

**Purpose** Use the monitoring functionality to view the Address Pools page.

**Action** To monitor Address Pools, select **Monitor>Access>Address Pools** in the J-Web user interface.

**Meaning** [Table 168](#) summarizes key output fields in the Address Pools page.

**Table 168: Address Pools Monitoring Page**

| Field                          | Values                                                                        | Additional Information |
|--------------------------------|-------------------------------------------------------------------------------|------------------------|
| <b>Address Pool Properties</b> |                                                                               |                        |
| Address Pool Name              | Displays the name of the address pool.                                        | -                      |
| Network Address                | Displays the IP network address of the address pool.                          | -                      |
| Address Ranges                 | Displays the name, the lower limit, and the upper limit of the address range. | -                      |

Table 168: Address Pools Monitoring Page (*continued*)

| Field                                  | Values                                                    | Additional Information                                                                 |
|----------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------|
| Primary DNS                            | Displays the primary-dns IP address.                      | -                                                                                      |
| Secondary DNS                          | Displays the secondary-dns IP address.                    | -                                                                                      |
| Primary WINS                           | Displays the primary-wins IP address.                     | -                                                                                      |
| Secondary WINS                         | Displays the secondary-wins IP address.                   | -                                                                                      |
| <b>Address Pool Address Assignment</b> |                                                           |                                                                                        |
| IP Address                             | Displays the IP address of the address pool.              | -                                                                                      |
| Hardware Address                       | Displays the hardware MAC address of the address pool.    | -                                                                                      |
| Host/User                              | Displays the user name using the address pool.            | -                                                                                      |
| Type                                   | Displays the authentication type used by the address pool | The authentication types can be extended authentication (XAuth) or IKE Authentication. |

- Related Documentation**
- [Monitoring Interfaces on page 1794](#)
  - [Threats Monitoring Report on page 1859](#)

## Monitoring Ethernet Switching

**Purpose** View information about the Ethernet Switching interface details.

**Action** Select **Monitor>Switching>Ethernet Switching** in the J-Web user interface, or enter the following CLI commands:

- **show ethernet-switching table**
- **show ethernet-switching mac-learning-log**

Table 169 summarizes the Ethernet Switching output fields.

Table 169: Summary of Ethernet Switching Output Fields

| Field | Values                                            | Additional Information |
|-------|---------------------------------------------------|------------------------|
| VLAN  | The VLAN for which Ethernet Switching is enabled. | -                      |



Table 169: Summary of Ethernet Switching Output Fields (*continued*)

| Field       | Values                                                                                                                                                                                                                                                                                             | Additional Information |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| MAC Address | The MAC address associated with the VLAN. If a VLAN range has been configured for a VLAN, the output displays the MAC addresses for the entire series of VLANs that were created with that name.                                                                                                   | -                      |
| Type        | The type of MAC address. Values are: <ul style="list-style-type: none"> <li>static—The MAC address is manually created.</li> <li>learn—The MAC address is learned dynamically from a packet's source MAC address.</li> <li>flood—The MAC address is unknown and flooded to all members.</li> </ul> | -                      |
| Age         | The time remaining before the entry ages out and is removed from the Ethernet switching table.                                                                                                                                                                                                     | -                      |
| Interfaces  | Interface associated with learned MAC addresses or All-members (flood entry).                                                                                                                                                                                                                      | -                      |
| VLAN-ID     | The VLAN ID.                                                                                                                                                                                                                                                                                       | -                      |
| MAC Address | The learned MAC address.                                                                                                                                                                                                                                                                           | -                      |
| Time        | Timestamp when the MAC address was added or deleted from the log.                                                                                                                                                                                                                                  | -                      |
| State       | Indicates the MAC address learned on the interface.                                                                                                                                                                                                                                                | -                      |

**Related Documentation**

- [Monitoring Overview on page 1397](#)
- [Monitoring Interfaces on page 1794](#)

## Monitoring GVRP

**Purpose** Use the monitoring functionality to view the GVRP page.

**Action** To monitor GVRP select **Monitor>Switching>GVRP** in the J-Web user interface.

**Meaning** [Table 170](#) summarizes key output fields in the GVRP page.

Table 170: GVRP Monitoring Page

| Field                     | Value                                         | Additional Information |
|---------------------------|-----------------------------------------------|------------------------|
| Global GVRP Configuration |                                               |                        |
| GVRP Status               | Displays whether GVRP is enabled or disabled. | —                      |

Table 170: GVRP Monitoring Page (*continued*)

| Field                         | Value                                                                                                                                                                 | Additional Information |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| GVRP Timer                    | Displays the GVRP timer in millisecond.                                                                                                                               | —                      |
| Join                          | The number of milliseconds the interfaces must wait before sending VLAN advertisements.                                                                               | —                      |
| Leave                         | The number of milliseconds an interface must wait after receiving a Leave message to remove the interface from the VLAN specified in the message.                     | —                      |
| Leave All                     | The interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages maintain current GVRP VLAN membership information in the network. | —                      |
| <b>GVRP Interface Details</b> |                                                                                                                                                                       |                        |
| Interface Name                | The interface on which GVRP is configured.                                                                                                                            | —                      |
| Protocol Status               | Displays whether GVRP is enabled or disabled.                                                                                                                         | —                      |

- Related Documentation**
- [Monitoring Ethernet Switching on page 1792](#)
  - [Monitoring Spanning Tree on page 1805](#)

## Monitoring Interfaces

**Purpose** View general information about all physical and logical interfaces for a device.

**Action** Select **Monitor>Interfaces** in the J-Web user interface. The J-Web Interfaces page displays the following details about each device interface:

- Port—Indicates the interface name.
- Admin Status—Indicates whether the interface is enabled (Up) or disabled (Down).
- Link Status—Indicates whether the interface is linked (Up) or not linked (Down).
- Address—Indicates the IP address of the interface.
- Zone—Indicates whether the zone is an untrust zone or a trust zone.
- Services—Indicates services that are enabled on the device, such as HTTP and SSH.
- Protocols—Indicates protocols that are enabled on the device, such as BGP and IGMP.
- Input Rate graph—Displays interface bandwidth utilization. Input rates are shown in bytes per second.

- Output Rate graph—Displays interface bandwidth utilization. Output rates are shown in bytes per second.
- Error Counters chart—Displays input and output error counters in the form of a bar chart.
- Packet Counters chart—Displays the number of broadcast, unicast, and multicast packet counters in the form of a pie chart. (Packet counter charts are supported only for interfaces that support MAC statistics.)

To change the interface display, use the following options:

- Port for FPC—Controls the member for which information is displayed.
- Start/Stop button—Starts or stops monitoring the selected interfaces.
- Show Graph—Displays input and output packet counters and error counters in the form of charts.
- Pop-up button—Displays the interface graphs in a separate pop-up window.
- Details—Displays extensive statistics about the selected interface, including its general status, traffic information, IP address, I/O errors, class-of-service data, and statistics.
- Refresh Interval—Indicates the duration of time after which you want the data on the page to be refreshed.
- Clear Statistics—Clears the statistics for the selected interface.

Alternatively, you can enter the following **show** commands in the CLI to view interface status and traffic statistics:

- **show interfaces terse**



**NOTE:** On SRX Series devices, on configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

- **show interfaces detail**
- **show interfaces extensive**
- **show interfaces *interface-name***

## Monitoring MPLS Traffic Engineering Information

This section contains the following topics:

- [Monitoring MPLS Interfaces on page 1796](#)
- [Monitoring MPLS LSP Information on page 1796](#)
- [Monitoring MPLS LSP Statistics on page 1797](#)

- [Monitoring RSVP Session Information on page 1798](#)
- [Monitoring MPLS RSVP Interfaces Information on page 1799](#)

## Monitoring MPLS Interfaces

**Purpose** View the interfaces on which MPLS is configured, including operational state and any administrative groups applied to an interface.

**Action** Select **Monitor>MPLS>Interfaces** in the J-Web user interface, or enter the **show mpls interface** command.

[Table 171](#) summarizes key output fields in the MPLS interface information display.

**Table 171: Summary of Key MPLS Interface Information Output Fields**

| Field                 | Values                                                                         | Additional Information |
|-----------------------|--------------------------------------------------------------------------------|------------------------|
| Interface             | Name of the interface on which MPLS is configured.                             | —                      |
| State                 | State of the specified interface: <b>Up</b> or <b>Dn</b> (down).               | —                      |
| Administrative groups | Administratively assigned colors of the MPLS link configured on the interface. | —                      |

## Monitoring MPLS LSP Information

**Purpose** View all label-switched paths (LSPs) configured on the services router, including all inbound (ingress), outbound (egress), and transit LSP information.

**Action** Select **Monitor>MPLS>LSP Information** in the J-Web user interface, or enter the **show mpls lsp** command.

[Table 172](#) summarizes key output fields in the MPLS LSP information display.

**Table 172: Summary of Key MPLS LSP Information Output Fields**

| Field       | Values                                                                                  | Additional Information                                                                                       |
|-------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Ingress LSP | Information about LSPs on the inbound device. Each session has one line of output.      | —                                                                                                            |
| Egress LSP  | Information about the LSPs on the outbound device. Each session has one line of output. | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| Transit LSP | Number of LSPs on the transit routers and the state of these paths.                     | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| To          | Destination (outbound device) of the session.                                           | —                                                                                                            |

Table 172: Summary of Key MPLS LSP Information Output Fields (*continued*)

| Field       | Values                                                                                                                                                                                                                                             | Additional Information                                                                                                                                                                           |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| From        | Source (inbound device) of the session.                                                                                                                                                                                                            | —                                                                                                                                                                                                |
| State       | State of the path. It can be <b>Up</b> , <b>Down</b> , or <b>AdminDn</b> .                                                                                                                                                                         | <b>AdminDn</b> indicates that the LSP is being taken down gracefully.                                                                                                                            |
| Rt          | Number of active routes (prefixes) installed in the routing table.                                                                                                                                                                                 | For inbound RSVP sessions, the routing table is the primary IPv4 table ( <b>inet.0</b> ). For transit and outbound RSVP sessions, the routing table is the primary MPLS table ( <b>mpls.0</b> ). |
| Active Path | Name of the active path: <b>Primary</b> or <b>Secondary</b> .                                                                                                                                                                                      | This field is used for inbound LSPs only.                                                                                                                                                        |
| P           | An asterisk (*) in this column indicates that the LSP is a primary path.                                                                                                                                                                           | This field is used for inbound LSPs only.                                                                                                                                                        |
| LSPname     | Configured name of the LSP.                                                                                                                                                                                                                        | —                                                                                                                                                                                                |
| Style       | RSVP reservation style. This field consists of two parts. The first is the number of active reservations. The second is the reservation style, which can be <b>FF</b> (fixed filter), <b>SE</b> (shared explicit), or <b>WF</b> (wildcard filter). | This field is used for outbound and transit LSPs only.                                                                                                                                           |
| Labelin     | Incoming label for this LSP.                                                                                                                                                                                                                       | —                                                                                                                                                                                                |
| Labelout    | Outgoing label for this LSP.                                                                                                                                                                                                                       | —                                                                                                                                                                                                |
| Total       | Total number of LSPs displayed for the particular type— <b>ingress</b> (inbound), <b>egress</b> (outbound), or <b>transit</b> .                                                                                                                    | —                                                                                                                                                                                                |

## Monitoring MPLS LSP Statistics

**Purpose** Display statistics for LSP sessions currently active on the device, including the total number of packets and bytes forwarded through an LSP.

**Action** Select **Monitor>MPLS>LSP Statistics** in the J-Web user interface, or enter the **show mpls lsp statistics** command.



**NOTE:** Statistics are not available for LSPs on the outbound device, because the penultimate device in the LSP sets the label to 0. Also, as the packet arrives at the outbound device, the hardware removes its MPLS header and the packet reverts to being an IPv4 packet. Therefore, it is counted as an IPv4 packet, not an MPLS packet.

Table 173 summarizes key output fields in the MPLS LSP statistics display.

**Table 173: Summary of Key MPLS LSP Statistics Output Fields**

| Field       | Values                                                                                                                          | Additional Information                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Ingress LSP | Information about LSPs on the inbound device. Each session has one line of output.                                              | —                                                                                                            |
| Egress LSP  | Information about the LSPs on the outbound device. Each session has one line of output.                                         | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| Transit LSP | Number of LSPs on the transit routers and the state of these paths.                                                             | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| To          | Destination (outbound device) of the session.                                                                                   | —                                                                                                            |
| From        | Source (inbound device) of the session.                                                                                         | —                                                                                                            |
| State       | State of the path: <b>Up</b> , <b>Down</b> , or <b>AdminDn</b> .                                                                | <b>AdminDn</b> indicates that the LSP is being taken down gracefully.                                        |
| Packets     | Total number of packets received on the LSP from the upstream neighbor.                                                         | —                                                                                                            |
| Bytes       | Total number of bytes received on the LSP from the upstream neighbor.                                                           | —                                                                                                            |
| LSPname     | Configured name of the LSP.                                                                                                     | —                                                                                                            |
| Total       | Total number of LSPs displayed for the particular type— <b>ingress</b> (inbound), <b>egress</b> (outbound), or <b>transit</b> . | —                                                                                                            |

## Monitoring RSVP Session Information

**Purpose** View information about RSVP-signaled LSP sessions currently active on the device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.

**Action** Select **Monitor>MPLS>RSVP Sessions** in the J-Web user interface, or enter the **show rsvp session** command.

Table 174 summarizes key output fields in the RSVP session information display.

**Table 174: Summary of Key RSVP Session Information Output Fields**

| Field       | Values                                                                        | Additional Information |
|-------------|-------------------------------------------------------------------------------|------------------------|
| Ingress LSP | Information about inbound RSVP sessions. Each session has one line of output. | —                      |

Table 174: Summary of Key RSVP Session Information Output Fields (*continued*)

| Field       | Values                                                                                                                                                                                                                                             | Additional Information                                                                                                                                                                           |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Egress LSP  | Information about outbound RSVP sessions. Each session has one line of output.                                                                                                                                                                     | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.                                                                                     |
| Transit LSP | Information about transit RSVP sessions.                                                                                                                                                                                                           | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.                                                                                     |
| To          | Destination (outbound device) of the session.                                                                                                                                                                                                      | —                                                                                                                                                                                                |
| From        | Source (inbound device) of the session.                                                                                                                                                                                                            | —                                                                                                                                                                                                |
| State       | State of the path: <b>Up</b> , <b>Down</b> , or <b>AdminDn</b> .                                                                                                                                                                                   | <b>AdminDn</b> indicates that the LSP is being taken down gracefully.                                                                                                                            |
| Rt          | Number of active routes (prefixes) installed in the routing table.                                                                                                                                                                                 | For inbound RSVP sessions, the routing table is the primary IPv4 table ( <b>inet.0</b> ). For transit and outbound RSVP sessions, the routing table is the primary MPLS table ( <b>mpls.0</b> ). |
| Style       | RSVP reservation style. This field consists of two parts. The first is the number of active reservations. The second is the reservation style, which can be <b>FF</b> (fixed filter), <b>SE</b> (shared explicit), or <b>WF</b> (wildcard filter). | This field is used for outbound and transit LSPs only.                                                                                                                                           |
| Labelin     | Incoming label for this RSVP session.                                                                                                                                                                                                              | —                                                                                                                                                                                                |
| Labelout    | Outgoing label for this RSVP session.                                                                                                                                                                                                              | —                                                                                                                                                                                                |
| LSPname     | Configured name of the LSP.                                                                                                                                                                                                                        | —                                                                                                                                                                                                |
| Total       | Total number of RSVP sessions displayed for the particular type— <b>ingress</b> (inbound), <b>egress</b> (outbound), or <b>transit</b> .                                                                                                           | —                                                                                                                                                                                                |

## Monitoring MPLS RSVP Interfaces Information

**Purpose** View information about the interfaces on which RSVP is enabled, including the interface name, total bandwidth through the interface, and total current reserved and reservable (available) bandwidth on the interface.

**Action** Select **Monitor>MPLS>RSVP Interfaces** in the J-Web user interface, or enter the **show rsvp interface** command.

Table 175 summarizes key output fields in the RSVP interfaces information display.

Table 175: Summary of Key RSVP Interfaces Information Output Fields

| Field          | Values                                                                                                                                                                                                                                                                                                                       | Additional Information |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| RSVP Interface | Number of interfaces on which RSVP is active. Each interface has one line of output.                                                                                                                                                                                                                                         | —                      |
| Interface      | Name of the interface.                                                                                                                                                                                                                                                                                                       | —                      |
| State          | State of the interface: <ul style="list-style-type: none"> <li>• <b>Disabled</b>—No traffic engineering information is displayed.</li> <li>• <b>Down</b>—The interface is not operational.</li> <li>• <b>Enabled</b>—Displays traffic engineering information.</li> <li>• <b>Up</b>—The interface is operational.</li> </ul> | —                      |
| Active resv    | Number of reservations that are actively reserving bandwidth on the interface.                                                                                                                                                                                                                                               | —                      |
| Subscription   | User-configured subscription factor.                                                                                                                                                                                                                                                                                         | —                      |
| Static BW      | Total interface bandwidth, in bits per second (bps).                                                                                                                                                                                                                                                                         | —                      |
| Available BW   | Amount of bandwidth that RSVP is allowed to reserve, in bits per second (bps). It is equal to <b>(static bandwidth X subscription factor)</b> .                                                                                                                                                                              | —                      |
| Reserved BW    | Currently reserved bandwidth, in bits per second (bps).                                                                                                                                                                                                                                                                      | —                      |
| Highwater mark | Highest bandwidth that has ever been reserved on this interface, in bits per second (bps).                                                                                                                                                                                                                                   | —                      |

- Related Documentation**
- [Configuring Ping MPLS on page 1911](#)
  - [MPLS Connection Checking Overview on page 1909](#)
  - [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring PPP

- Purpose** Display PPP monitoring information, including PPP address pool information, session status for PPP interfaces, cumulative statistics for all PPP interfaces, and a summary of PPP sessions.





**NOTE:** PPP monitoring information is available only in the CLI. The J-Web user interface does not include pages for displaying PPP monitoring information.

**Action** Enter the following CLI commands:

- `show ppp address-pool pool-name`
- `show ppp interface interface-name`
- `show ppp statistics`
- `show ppp summary`

**Related Documentation**

- [Monitoring Overview on page 1397](#)
- [Monitoring Interfaces on page 1794](#)

## Monitoring PPPoE

**Purpose** Display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the device, and the PPPoE version configured on the device.

**Action** Select **Monitor>PPPoE** in the J-Web user interface. To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

[Table 176](#) summarizes key output fields in PPPoE displays.

**Table 176: Summary of Key PPPoE Output Fields**

| Field                   | Values                                           | Additional Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PPPoE Interfaces</b> |                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Interface               | Name of the PPPoE interface.                     | Click the interface name to display PPPoE information for the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| State                   | State of the PPPoE session on the interface.     | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session ID              | Unique session identifier for the PPPoE session. | To establish a PPPoE session, first the device acting as a PPPoE client obtains the Ethernet address of the PPPoE server or access concentrator, and then the client and the server negotiate a unique session ID. This process is referred to as PPPoE active discovery and is made up of four steps: initiation, offer, request, and session confirmation. The access concentrator generates the session ID for session confirmation and sends it to the PPPoE client in a PPPoE Active Discovery Session-Confirmation (PADS) packet. |

Table 176: Summary of Key PPPoE Output Fields (*continued*)

| Field                   | Values                                                                                                              | Additional Information                                                                                                                                                  |
|-------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Name            | Type of service required from the access concentrator.                                                              | Service Name identifies the type of service provided by the access concentrator, such as the name of the Internet service provider (ISP), class, or quality of service. |
| Configured AC Name      | Configured access concentrator name.                                                                                | —                                                                                                                                                                       |
| Session AC Names        | Name of the access concentrator.                                                                                    | —                                                                                                                                                                       |
| AC MAC Address          | Media access control (MAC) address of the access concentrator.                                                      | —                                                                                                                                                                       |
| Session Uptime          | Number of seconds the current PPPoE session has been running.                                                       | —                                                                                                                                                                       |
| Auto-Reconnect Timeout  | Number of seconds to wait before reconnecting after a PPPoE session is terminated.                                  | —                                                                                                                                                                       |
| Idle Timeout            | Number of seconds a PPPoE session can be idle without disconnecting.                                                | —                                                                                                                                                                       |
| Underlying Interface    | Name of the underlying logical Ethernet or ATM interface on which PPPoE is running—for example, <b>ge-0/0/0.1</b> . | —                                                                                                                                                                       |
| <b>PPPoE Statistics</b> |                                                                                                                     |                                                                                                                                                                         |
| Active PPPoE Sessions   | Total number of active PPPoE sessions.                                                                              | —                                                                                                                                                                       |

Table 176: Summary of Key PPPoE Output Fields (*continued*)

| Field                | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Additional Information |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Packet Type          | Packets sent and received during the PPPoE session, categorized by packet type and packet error: <ul style="list-style-type: none"> <li>• <b>PADI</b>—PPPoE Active Discovery Initiation packets.</li> <li>• <b>PADO</b>—PPPoE Active Discovery Offer packets.</li> <li>• <b>PADR</b>—PPPoE Active Discovery Request packets.</li> <li>• <b>PADS</b>—PPPoE Active Discovery Session-Confirmation packets.</li> <li>• <b>PADT</b>—PPPoE Active Discovery Terminate packets.</li> <li>• <b>Service Name Error</b>—Packets for which the Service-Name request could not be honored.</li> <li>• <b>AC System Error</b>—Packets for which the access concentrator experienced an error in processing the host request. For example, the host had insufficient resources to create a virtual circuit.</li> <li>• <b>Generic Error</b>—Packets that indicate an unrecoverable error occurred.</li> <li>• <b>Malformed Packet</b>—Malformed or short packets that caused the packet handler to disregard the frame as unreadable.</li> <li>• <b>Unknown Packet</b>—Unrecognized packets.</li> </ul> | —                      |
| Sent                 | Number of the specific type of packet sent from the PPPoE client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | —                      |
| Received             | Number of the specific type of packet received by the PPPoE client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | —                      |
| Timeout              | Information about the timeouts that occurred during the PPPoE session. <ul style="list-style-type: none"> <li>• <b>PADI</b>—Number of timeouts that occurred for the PADI packet.</li> <li>• <b>PADO</b>—Number of timeouts that occurred for the PADO packet. (This value is always 0 and is not supported.)</li> <li>• <b>PADR</b>—Number of timeouts that occurred for the PADR packet.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —                      |
| Sent                 | Number of the timeouts that occurred for PADI, PADO, and PADR packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |
| <b>PPPoE Version</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                        |
| Maximum Sessions     | Maximum number of active PPPoE sessions the device can support. The default is 256 sessions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | —                      |

Table 176: Summary of Key PPPoE Output Fields (*continued*)

| Field                         | Values                                                                                                                                                                           | Additional Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PADI Resend Timeout           | Initial time, (in seconds) the device waits to receive a PADO packet for the PADI packet sent—for example, 2 seconds. This timeout doubles for each successive PADI packet sent. | The PPPoE Active Discovery Initiation (PADI) packet is sent to the access concentrator to initiate a PPPoE session. Typically, the access concentrator responds to a PADI packet with a PPPoE Active Discovery Offer (PADO) packet. If the access concentrator does not send a PADO packet, the device sends the PADI packet again after timeout period is elapsed. The PADI Resend Timeout doubles for each successive PADI packet sent. For example, if the PADI Resend Timeout is 2 seconds, the second PADI packet is sent after 2 seconds, the third after 4 seconds, the fourth after 8 seconds, and so on. |
| PADR Resend Timeout           | Initial time (in seconds) the device waits to receive a PADS packet for the PADR packet sent. This timeout doubles for each successive PADR packet sent.                         | The PPPoE Active Discovery Request (PADR) packet is sent to the access concentrator in response to a PADO packet, and to obtain the PPPoE session ID. Typically, the access concentrator responds to a PADR packet with a PPPoE Active Discovery Session-Confirmation (PADS) packet, which contains the session ID. If the access concentrator does not send a PADS packet, the device sends the PADR packet again after the PADR Resend Timeout period is elapsed. The PADR Resend Timeout doubles for each successive PADR packet sent.                                                                         |
| Maximum Resend Timeout        | Maximum value (in seconds) that the PADI or PADR resend timer can accept—for example, 64 seconds. The maximum value is 64.                                                       | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Maximum Configured AC Timeout | Time (in seconds), within which the configured access concentrator must respond.                                                                                                 | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Alternatively, enter the following CLI commands:

- **show pppoe interfaces**
- **show pppoe statistics**
- **show pppoe version**

You can also view status information about the PPPoE interface by entering the **show interfaces pp0** command in the CLI editor.

#### Related Documentation

- [Monitoring Overview on page 1397](#)
- [Monitoring Interfaces on page 1794](#)
- [Monitoring DHCP Client Bindings on page 1845](#)

## Monitoring Spanning Tree

**Purpose** Use the monitoring functionality to view the Spanning Tree page.

**Action** To monitor spanning tree, select **Monitor>Switching>Spanning Tree** in the J-Web user interface.

**Meaning** [Table 177](#) summarizes key output fields in the spanning tree page.

**Table 177: Spanning Tree Monitoring Page**

| Field                      | Value                                                                                  | Additional Information                                                                      |
|----------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Bridge parameters</b>   |                                                                                        |                                                                                             |
| Context ID                 | An internally generated identifier.                                                    | —                                                                                           |
| Enabled Protocol           | Spanning tree protocol type enabled.                                                   | —                                                                                           |
| Root ID                    | Bridge ID of the elected spanning tree root bridge.                                    | The bridge ID consists of a configurable bridge priority and the MAC address of the bridge. |
| Bridge ID                  | Locally configured bridge ID.                                                          | —                                                                                           |
| Inter instance ID          | An internally generated instance identifier.                                           | —                                                                                           |
| Extended system ID         | Extended system generated instance identifier.                                         | —                                                                                           |
| Maximum age                | Maximum age of received bridge protocol data units (BPDUs).                            | —                                                                                           |
| Number of topology changes | Total number of STP topology changes detected since the switch last booted.            | —                                                                                           |
| Forward delay              | Spanning tree forward delay.                                                           | —                                                                                           |
| <b>Interface List</b>      |                                                                                        |                                                                                             |
| Interface Name             | Interface configured to participate in the STP instance.                               | —                                                                                           |
| Port ID                    | Logical interface identifier configured to participate in the STP instance.            | —                                                                                           |
| Designated Port ID         | Port ID of the designated port for the LAN segment to which the interface is attached. | —                                                                                           |
| Port Cost                  | Configured cost for the interface.                                                     | —                                                                                           |
| State                      | STP port state. Forwarding (FWD), blocking (BLK), listening, learning, or disabled.    | —                                                                                           |

Table 177: Spanning Tree Monitoring Page (*continued*)

| Field | Value                                                                               | Additional Information |
|-------|-------------------------------------------------------------------------------------|------------------------|
| Role  | MSTP or RSTP port role. Designated (DESG), backup (BKUP), alternate (ALT), or root. | –                      |

- Related Documentation**
- [Monitoring Ethernet Switching on page 1792](#)
  - [Monitoring GVRP on page 1793](#)

## Monitoring the WAN Acceleration Interface

**Purpose** View status information and traffic statistics for the WAN acceleration interface.

**Action** Select **Monitor>WAN Acceleration** in the J-Web user interface, or select **Monitor>Interfaces** and select the interface name (**wx-slot/0/0**). Alternatively, enter the following CLI command:

```
[edit]
user@host# show interfaces wx-slot/0/0 detail
```

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

# Monitoring NAT

- [Monitoring NAT on page 1807](#)

## Monitoring NAT

This section contains the following topics:

- [Monitoring Source NAT Information on page 1807](#)
- [Monitoring Destination NAT Information on page 1813](#)
- [Monitoring Static NAT Information on page 1815](#)
- [Monitoring Incoming Table Information on page 1816](#)
- [Monitoring Interface NAT Port Information on page 1817](#)

### Monitoring Source NAT Information

**Purpose** Display configured information about source Network Address Translation (NAT) rules, pools, persistent NAT, and paired addresses.

**Action** Select **Monitor>NAT>Source NAT** in the J-Web user interface, or enter the following CLI commands:

- **show security nat source summary**
- **show security nat source pool *pool-name***
- **show security nat source persistent-nat-table**
- **show security nat source paired-address**

[Table 178](#) describes the available options for monitoring source NAT.

Table 178: Source NAT Monitoring Page

| Field         | Description                 | Action                                                                |
|---------------|-----------------------------|-----------------------------------------------------------------------|
| Rules         |                             |                                                                       |
| Rule-set Name | Name of the rule set.       | Select all rule sets or a specific rule set to display from the list. |
| Total rules   | Number of rules configured. | —                                                                     |

Table 178: Source NAT Monitoring Page (*continued*)

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                   | Action |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| ID                                     | Rule ID number.                                                                                                                                                                                                                                                                                                                               | —      |
| Name                                   | Name of the rule .                                                                                                                                                                                                                                                                                                                            | —      |
| From                                   | Name of the routing instance/zone/interface from which the packet flows.                                                                                                                                                                                                                                                                      | —      |
| To                                     | Name of the routing instance/zone/interface to which the packet flows.                                                                                                                                                                                                                                                                        | —      |
| Source address range                   | Source IP address range in the source pool.                                                                                                                                                                                                                                                                                                   | —      |
| Destination address range              | Destination IP address range in the source pool.                                                                                                                                                                                                                                                                                              | —      |
| Source ports                           | Source port numbers.                                                                                                                                                                                                                                                                                                                          | —      |
| Ip protocol                            | IP protocol.                                                                                                                                                                                                                                                                                                                                  | —      |
| Action                                 | Action taken for a packet that matches a rule.                                                                                                                                                                                                                                                                                                | —      |
| Persistent NAT type                    | Persistent NAT type.                                                                                                                                                                                                                                                                                                                          | —      |
| Inactivity timeout                     | Inactivity timeout interval for the persistent NAT binding.                                                                                                                                                                                                                                                                                   | —      |
| Alarm threshold                        | Utilization alarm threshold.                                                                                                                                                                                                                                                                                                                  | —      |
| Max session number                     | The maximum number of sessions.                                                                                                                                                                                                                                                                                                               | —      |
| Sessions (Succ/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>Succ—Number of successful session installations after the NAT rule is matched.</li> <li>Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>Current—Number of sessions that reference the specified rule.</li> </ul> | —      |
| Translation Hits                       | Number of times a translation in the translation table is used for a source NAT rule.                                                                                                                                                                                                                                                         | —      |



Table 178: Source NAT Monitoring Page (*continued*)

| Field                                  | Description                                                                    | Action                                                        |
|----------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Pools</b>                           |                                                                                |                                                               |
| Pool Name                              | The names of the pools.                                                        | Select all pools or a specific pool to display from the list. |
| Total Pools                            | Total pools added.                                                             | —                                                             |
| ID                                     | ID of the pool.                                                                | —                                                             |
| Name                                   | Name of the source pool.                                                       | —                                                             |
| Address range                          | IP address range in the source pool.                                           | —                                                             |
| Single/Twin ports                      | Number of allocated single and twin ports.                                     | —                                                             |
| Port                                   | Source port number in the pool.                                                | —                                                             |
| Address assignment                     | Displays the type of address assignment.                                       | —                                                             |
| Alarm threshold                        | Utilization alarm threshold.                                                   | —                                                             |
| Port overloading factor                | Port overloading capacity.                                                     | —                                                             |
| Routing instance                       | Name of the routing instance.                                                  | —                                                             |
| Total addresses                        | Total IP address, IP address set, or address book entry.                       | —                                                             |
| Host address base                      | Host base address of the original source IP address range.                     | —                                                             |
| Translation hits                       | Number of times a translation in the translation table is used for source NAT. | —                                                             |
| <b>Top 10 Translation Hits</b>         |                                                                                |                                                               |
| Graph                                  | Displays the graph of top 10 translation hits.                                 | —                                                             |
| <b>Persistent NAT</b>                  |                                                                                |                                                               |
| <b>Persistent NAT table statistics</b> |                                                                                |                                                               |
| binding total                          | Displays the total number of persistent NAT bindings for the FPC.              | —                                                             |

Table 178: Source NAT Monitoring Page (*continued*)

| Field                       | Description                                                                       | Action                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| binding in use              | Number of persistent NAT bindings that are in use for the FPC.                    | —                                                                          |
| enode total                 | Total number of persistent NAT enodes for the FPC.                                | —                                                                          |
| enode in use                | Number of persistent NAT enodes that are in use for the FPC.                      | —                                                                          |
| <b>Persistent NAT table</b> |                                                                                   |                                                                            |
| Source NAT pool             | Name of the pool.                                                                 | Select all pools or a specific pool to display from the list.              |
| Internal IP                 | Internal IP address.                                                              | Select all IP addresses or a specific IP address to display from the list. |
| Internal port               | Displays the internal ports configured in the system.                             | Select the port to display from the list.                                  |
| Internal protocol           | Internal protocols .                                                              | Select all protocols or a specific protocol to display from the list.      |
| Internal IP                 | Internal transport IP address of the outgoing session from internal to external.  | —                                                                          |
| Internal port               | Internal transport port number of the outgoing session from internal to external. | —                                                                          |
| Internal protocol           | Internal protocol of the outgoing session from internal to external.              | —                                                                          |
| Reflective IP               | Translated IP address of the source IP address.                                   | —                                                                          |
| Reflective port             | Displays the translated number of the port.                                       | —                                                                          |
| Reflective protocol         | Translated protocol.                                                              | —                                                                          |
| Source NAT pool             | Name of the source NAT pool where persistent NAT is used.                         | —                                                                          |
| Type                        | Persistent NAT type.                                                              | —                                                                          |
| Left time/Conf time         | Inactivity timeout period that remains and the configured timeout value.          | —                                                                          |

Table 178: Source NAT Monitoring Page (*continued*)

| Field                                   | Description                                                                                               | Action                                                                                                                                                                        |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current session num/Max session num     | Number of current sessions associated with the persistent NAT binding and the maximum number of sessions. | —                                                                                                                                                                             |
| Source NAT rule                         | Name of the source NAT rule to which this persistent NAT binding applies.                                 | —                                                                                                                                                                             |
| <b>External node table</b>              |                                                                                                           |                                                                                                                                                                               |
| Internal IP                             | Internal transport IP address of the outgoing session from internal to external.                          | —                                                                                                                                                                             |
| Internal port                           | Internal port number of the outgoing session from internal to external.                                   | —                                                                                                                                                                             |
| External IP                             | External IP address of the outgoing session from internal to external.                                    | —                                                                                                                                                                             |
| External port                           | External port of the outgoing session from internal to external.                                          | —                                                                                                                                                                             |
| Zone                                    | External zone of the outgoing session from internal to external.                                          | —                                                                                                                                                                             |
| <b>Paired Address</b>                   |                                                                                                           |                                                                                                                                                                               |
| Pool name                               | Name of the pool.                                                                                         | Select all pools or a specific pool to display from the list.                                                                                                                 |
| Specified Address                       | IP address.                                                                                               | Select all addresses, or select the internal or external IP address to display, and enter the IP address.                                                                     |
| Pool name                               | Displays the selected pool or pools.                                                                      | —                                                                                                                                                                             |
| Internal address                        | Displays the internal IP address.                                                                         | —                                                                                                                                                                             |
| External address                        | Displays the external IP address.                                                                         | —                                                                                                                                                                             |
| <b>Resource Usage</b>                   |                                                                                                           |                                                                                                                                                                               |
| <b>Utilization for all source pools</b> |                                                                                                           |                                                                                                                                                                               |
| Pool name                               | Name of the pool.                                                                                         | To view additional usage information for Port Address Translation (PAT) pools, select a pool name. The information displays under Detail Port Utilization for Specified Pool. |
| Pool type                               | Pool type: PAT or Non-PAT.                                                                                | —                                                                                                                                                                             |

Table 178: Source NAT Monitoring Page (*continued*)

| Field                                             | Description                                                                                                                                                                                                                      | Action                                                                          |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Port overloading factor                           | Port overloading capacity for PAT pools.                                                                                                                                                                                         | —                                                                               |
| Address                                           | Addresses in the pool.                                                                                                                                                                                                           | —                                                                               |
| Used                                              | Number of used resources in the pool.<br><br>For Non-PAT pools, the number of used IP addresses is displayed.<br><br>For PAT pools, the number of used ports is displayed.                                                       | —                                                                               |
| Available                                         | Number of available resources in the pool.<br><br>For Non-PAT pools, the number of available IP addresses is displayed.<br><br>For PAT pools, the number of available ports is displayed.                                        | —                                                                               |
| Total                                             | Number of used and available resources in the pool.<br><br>For Non-PAT pools, the total number of used and available IP addresses is displayed.<br><br>For PAT pools, the total number of used and available ports is displayed. | —                                                                               |
| Usage                                             | Percent of resources used.<br><br>For Non-PAT pools, the percent of IP addresses used is displayed.<br><br>For PAT pools, the percent of ports, including single and twin ports, is displayed.                                   | —                                                                               |
| Peak usage                                        | Percent of resources used during the peak date and time.                                                                                                                                                                         | —                                                                               |
| <b>Detail Port Utilization for Specified Pool</b> |                                                                                                                                                                                                                                  |                                                                                 |
| Address Name                                      | IP addresses in the PAT pool.                                                                                                                                                                                                    | Select the IP address for which you want to display detailed usage information. |
| Factor-Index                                      | Index number.                                                                                                                                                                                                                    | —                                                                               |
| Port-range                                        | Displays the number of ports allocated at a time.                                                                                                                                                                                | —                                                                               |
| Used                                              | Displays the number of used ports.                                                                                                                                                                                               | —                                                                               |
| Available                                         | Displays the number of available ports.                                                                                                                                                                                          | —                                                                               |

Table 178: Source NAT Monitoring Page (*continued*)

| Field | Description                                                          | Action |
|-------|----------------------------------------------------------------------|--------|
| Total | Displays the number of used and available ports.                     | —      |
| Usage | Displays the percentage of ports used during the peak date and time. | —      |

## Monitoring Destination NAT Information

**Purpose** View the destination Network Address Translation (NAT) summary table and the details of the specified NAT destination address pool information.

**Action** Select **Monitor>NAT> Destination NAT** in the J-Web user interface, or enter the following CLI commands:

- **show security nat destination summary**
- **show security nat destination pool *pool-name***

Table 179 summarizes key output fields in the destination NAT display.

Table 179: Summary of Key Destination NAT Output Fields

| Field                     | Values                                                                   | Action                                                                |
|---------------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Rules</b>              |                                                                          |                                                                       |
| Rule-set Name             | Name of the rule set.                                                    | Select all rule sets or a specific rule set to display from the list. |
| Total rules               | Number of rules configured.                                              | —                                                                     |
| ID                        | Rule ID number.                                                          | —                                                                     |
| Name                      | Name of the rule .                                                       | —                                                                     |
| Ruleset Name              | Name of the rule set.                                                    | —                                                                     |
| From                      | Name of the routing instance/zone/interface from which the packet flows. | —                                                                     |
| Source address range      | Source IP address range in the source pool.                              | —                                                                     |
| Destination address range | Destination IP address range in the source pool.                         | —                                                                     |

Table 179: Summary of Key Destination NAT Output Fields (*continued*)

| Field                                  | Values                                                                                                                                                                                                                                                                                                                                        | Action                                                        |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Destination port                       | Destination port in the destination pool.                                                                                                                                                                                                                                                                                                     | —                                                             |
| IP protocol                            | IP protocol.                                                                                                                                                                                                                                                                                                                                  | —                                                             |
| Action                                 | Action taken for a packet that matches a rule.                                                                                                                                                                                                                                                                                                | —                                                             |
| Alarm threshold                        | Utilization alarm threshold.                                                                                                                                                                                                                                                                                                                  | —                                                             |
| Sessions (Succ/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>Succ—Number of successful session installations after the NAT rule is matched.</li> <li>Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>Current—Number of sessions that reference the specified rule.</li> </ul> | —                                                             |
| Translation hits                       | Number of times a translation in the translation table is used for a destination NAT rule.                                                                                                                                                                                                                                                    | —                                                             |
| <b>Pools</b>                           |                                                                                                                                                                                                                                                                                                                                               |                                                               |
| Pool Name                              | The names of the pools.                                                                                                                                                                                                                                                                                                                       | Select all pools or a specific pool to display from the list. |
| Total Pools                            | Total pools added.                                                                                                                                                                                                                                                                                                                            | —                                                             |
| ID                                     | ID of the pool.                                                                                                                                                                                                                                                                                                                               | —                                                             |
| Name                                   | Name of the destination pool.                                                                                                                                                                                                                                                                                                                 | —                                                             |
| Address range                          | IP address range in the destination pool.                                                                                                                                                                                                                                                                                                     | —                                                             |
| Port                                   | Destination port number in the pool.                                                                                                                                                                                                                                                                                                          | —                                                             |
| Routing instance                       | Name of the routing instance.                                                                                                                                                                                                                                                                                                                 | —                                                             |
| Total addresses                        | Total IP address, IP address set, or address book entry.                                                                                                                                                                                                                                                                                      | —                                                             |
| Translation hits                       | Number of times a translation in the translation table is used for destination NAT.                                                                                                                                                                                                                                                           | —                                                             |
| <b>Top 10 Translation Hits</b>         |                                                                                                                                                                                                                                                                                                                                               |                                                               |
| Graph                                  | Displays the graph of top 10 translation hits.                                                                                                                                                                                                                                                                                                | —                                                             |

## Monitoring Static NAT Information

**Purpose** View static NAT rule information.

**Action** Select **Monitor>NAT>Static NAT** in the J-Web user interface, or enter the following CLI command:

**show security nat static rule**

Table 180 summarizes key output fields in the static NAT display.

**Table 180: Summary of Key Static NAT Output Fields**

| Field                 | Values                                                                        | Action                                                                |
|-----------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Rule-set Name         | Name of the rule set.                                                         | Select all rule sets or a specific rule set to display from the list. |
| Total rules           | Number of rules configured.                                                   | —                                                                     |
| ID                    | Rule ID number.                                                               | —                                                                     |
| Position              | Position of the rule that indicates the order in which it applies to traffic. | —                                                                     |
| Name                  | Name of the rule.                                                             | —                                                                     |
| Ruleset Name          | Name of the rule set.                                                         | —                                                                     |
| From                  | Name of the routing instance/interface/zone from which the packet comes       | —                                                                     |
| Source addresses      | Source IP addresses.                                                          | —                                                                     |
| Source ports          | Source port numbers.                                                          | —                                                                     |
| Destination addresses | Destination IP address and subnet mask.                                       | —                                                                     |
| Destination ports     | Destination port numbers .                                                    | —                                                                     |
| Host addresses        | Name of the host addresses.                                                   | —                                                                     |
| Host ports            | Host port numbers.                                                            | —                                                                     |
| Netmask               | Subnet IP address.                                                            | —                                                                     |
| Host routing instance | Name of the routing instance from which the packet comes.                     | —                                                                     |

Table 180: Summary of Key Static NAT Output Fields (*continued*)

| Field                                     | Values                                                                                                                                                                                                                                                                                                                                        | Action |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Alarm threshold                           | Utilization alarm threshold.                                                                                                                                                                                                                                                                                                                  | —      |
| Sessions<br>(Succ/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>Succ—Number of successful session installations after the NAT rule is matched.</li> <li>Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>Current—Number of sessions that reference the specified rule.</li> </ul> | —      |
| Translation hits                          | Number of times a translation in the translation table is used for a static NAT rule.                                                                                                                                                                                                                                                         | —      |
| <b>Top 10 Translation Hits</b>            |                                                                                                                                                                                                                                                                                                                                               |        |
| Graph                                     | Displays the graph of top 10 translation hits.                                                                                                                                                                                                                                                                                                | —      |

## Monitoring Incoming Table Information

**Purpose** View NAT table information.

**Action** Select **Monitor>NAT>Incoming Table** in the J-Web user interface, or enter the following CLI command:

```
show security nat incoming-table
```

Table 181 summarizes key output fields in the incoming table display.

Table 181: Summary of Key Incoming Table Output Fields

| Field                   | Values                                                                        |
|-------------------------|-------------------------------------------------------------------------------|
| <b>Statistics</b>       |                                                                               |
| In use                  | Number of entries in the NAT table.                                           |
| Maximum                 | Maximum number of entries possible in the NAT table.                          |
| Entry allocation failed | Number of entries failed for allocation.                                      |
| <b>Incoming Table</b>   |                                                                               |
| Clear                   |                                                                               |
| Destination             | Destination IP address and port number.                                       |
| Host                    | Host IP address and port number that the destination IP address is mapped to. |
| References              | Number of sessions referencing the entry.                                     |



Table 181: Summary of Key Incoming Table Output Fields (*continued*)

| Field       | Values                                              |
|-------------|-----------------------------------------------------|
| Timeout     | Timeout, in seconds, of the entry in the NAT table. |
| Source-pool | Name of source pool where translation is allocated. |

## Monitoring Interface NAT Port Information

**Purpose** View port usage for an interface source pool information.

**Action** Select **Monitor>Firewall/NAT>Interface NAT** in the J-Web user interface, or enter the following CLI command:

- **show security nat interface-nat-ports**

Table 182 summarizes key output fields in the interface NAT display.

Table 182: Summary of Key Interface NAT Output Fields

| Field                              | Values                                                         | Additional Information |
|------------------------------------|----------------------------------------------------------------|------------------------|
| <b>Interface NAT Summary Table</b> |                                                                |                        |
| Pool Index                         | Port pool index.                                               | —                      |
| Total Ports                        | Total number of ports in a port pool.                          | —                      |
| Single Ports Allocated             | Number of ports allocated one at a time that are in use.       | —                      |
| Single Ports Available             | Number of ports allocated one at a time that are free for use. | —                      |
| Twin Ports Allocated               | Number of ports allocated two at a time that are in use.       | —                      |
| Twin Ports Available               | Number of ports allocated two at a time that are free for use. | —                      |

**Related Documentation**

- [Monitoring Overview on page 1397](#)
- [Monitoring Interfaces on page 1794](#)



# Monitoring Security Policies

- [Monitoring Policy Statistics on page 1819](#)
- [Monitoring Routing Information on page 1820](#)
- [Monitoring Security Events by Policy on page 1827](#)
- [Monitoring Security Features on page 1829](#)

## Monitoring Policy Statistics

---

**Purpose** Monitor and record traffic that Junos OS permits or denies based on previously configured policies.

**Action** To monitor traffic, enable the count and log options.

**Count**—Configurable in an individual policy. If count is enabled, statistics are collected for sessions that enter the device for a given policy, and for the number of packets and bytes that pass through the device in both directions for a given policy. For counts (only for packets and bytes), you can specify that alarms be generated whenever the traffic exceeds specified thresholds. See [count \(Security Policies\)](#).

**Log**—Logging capability can be enabled with security policies during session initialization (**session-init**) or session close (**session-close**) stage. See [log \(Security Policies\)](#).

- To view logs from denied connections, enable log on **session-init**.
- To log sessions after their conclusion/tear-down, enable log on **session-close**.



**NOTE:** Session log is enabled at real time in the flow code which impacts the user performance. If both **session-close** and **session-init** are enabled, performance is further degraded as compared to enabling **session-init** only.

---

For details about information collected for session logs, see [Information Provided in Session Log Entries for SRX Series Services Gateways](#).

- Related Documentation**
- [Security Policies Overview](#)
  - [Troubleshooting Security Policies on page 1964](#)

- [Checking a Security Policy Commit Failure on page 1964](#)
- [Verifying a Security Policy Commit on page 1965](#)
- [Debugging Policy Lookup on page 1965](#)

## Monitoring Routing Information

---

This section contains the following topics:

- [Monitoring Route Information on page 1820](#)
- [Monitoring RIP Routing Information on page 1822](#)
- [Monitoring OSPF Routing Information on page 1823](#)
- [Monitoring BGP Routing Information on page 1825](#)

### Monitoring Route Information

**Purpose** View information about the routes in a routing table, including destination, protocol, state, and parameter information.

**Action** Select **Monitor>Routing>Route Information** in the J-Web user interface, or enter the following CLI commands:

- **show route terse**
- **show route detail**



**NOTE:** When you use an HTTPS connection in the Microsoft Internet Explorer browser to save a report from this page in the J-Web interface, the error message "Internet Explorer was not able to open the Internet site" is displayed. This problem occurs because the Cache-Control: no cache HTTP header is added on the server side and Internet Explorer does not allow you to download the encrypted file with the Cache-Control: no cache HTTP header set in the response from the server.

As a workaround, refer to Microsoft Knowledge Base article 323308, which is available at this URL: <http://support.microsoft.com/kb/323308>. Also, you can alternatively use HTTP in the Internet Explorer browser or use HTTPS in the Mozilla Firefox browser to save a file from this page.

[Table 183](#) describes the different filters, their functions, and the associated actions.

[Table 184](#) summarizes key output fields in the routing information display.

Table 183: Filtering Route Messages

| Field               | Function                                                                                                                             | Your Action                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Destination Address | Specifies the destination address of the route.                                                                                      | Enter the destination address.                                  |
| Protocol            | Specifies the protocol from which the route was learned.                                                                             | Enter the protocol name.                                        |
| Next hop address    | Specifies the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it. | Enter the next hop address.                                     |
| Receive protocol    | Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.               | Enter the routing protocol.                                     |
| Best route          | Specifies only the best route available.                                                                                             | Select the view details of the best route.                      |
| Inactive routes     | Specifies the inactive routes.                                                                                                       | Select the view details of inactive routes.                     |
| Exact route         | Specifies the exact route.                                                                                                           | Select the view details of the exact route.                     |
| Hidden routes       | Specifies the hidden routes.                                                                                                         | Select the view details of hidden routes.                       |
| Search              | Applies the specified filter and displays the matching messages.                                                                     | To apply the filter and display messages, click <b>Search</b> . |
| Reset               | Resets selected options to default                                                                                                   | To reset the filter, click <b>Reset</b> .                       |

Table 184: Summary of Key Routing Information Output Fields

| Field                  | Values                                                                                                                          | Additional Information                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Static Route Addresses | The list of static route addresses.                                                                                             | —                                                                    |
| Protocol               | Protocol from which the route was learned: <b>Static</b> , <b>Direct</b> , <b>Local</b> , or the name of a particular protocol. | —                                                                    |
| Preference             | The preference is the individual preference value for the route.                                                                | The route preference is used as one of the route selection criteria. |

Table 184: Summary of Key Routing Information Output Fields (*continued*)

| Field    | Values                                                                                                                                                                                                                                                                     | Additional Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Next-Hop | Network Layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.                                                                                                                                                     | <p>If a next hop is listed as <b>Discard</b>, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the <b>discard</b> attribute has been set.</p> <p>If a next hop is listed as <b>Reject</b>, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected.</p> <p>If a next hop is listed as <b>Local</b>, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).</p> |
| Age      | How long the route has been active.                                                                                                                                                                                                                                        | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| State    | Flags for this route.                                                                                                                                                                                                                                                      | There are many possible flags.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| AS Path  | <p>AS path through which the route was learned. The letters of the AS path indicate the path origin:</p> <ul style="list-style-type: none"> <li>• <b>I</b>—IGP.</li> <li>• <b>E</b>—EGP.</li> <li>• <b>?</b>—Incomplete. Typically, the AS path was aggregated.</li> </ul> | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Monitoring RIP Routing Information

**Purpose** View RIP routing information, including a summary of RIP neighbors and statistics.

**Action** Select **Monitor>Routing>RIP Information** in the J-Web user interface, or enter the following CLI commands:

- **show rip statistics**
- **show rip neighbors**

[Table 185](#) summarizes key output fields in the RIP routing display in the J-Web user interface.

Table 185: Summary of Key RIP Routing Output Fields

| Field                 | Values                            | Additional Information |
|-----------------------|-----------------------------------|------------------------|
| <b>RIP Statistics</b> |                                   |                        |
| Protocol Name         | The RIP protocol name.            | —                      |
| Port number           | The port on which RIP is enabled. | —                      |

Table 185: Summary of Key RIP Routing Output Fields (*continued*)

| Field                    | Values                                                                                 | Additional Information                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Hold down time           | The interval during which routes are neither advertised nor updated.                   | —                                                                                                                     |
| Global routes learned    | Number of RIP routes learned on the logical interface.                                 | —                                                                                                                     |
| Global routes held down  | Number of RIP routes that are not advertised or updated during the hold-down interval. | —                                                                                                                     |
| Global request dropped   | Number of requests dropped.                                                            | —                                                                                                                     |
| Global responses dropped | Number of responses dropped.                                                           | —                                                                                                                     |
| <b>RIP Neighbors</b>     |                                                                                        |                                                                                                                       |
| Details                  | Tab used to view the details of the interface on which RIP is enabled.                 | —                                                                                                                     |
| Neighbor                 | Name of the RIP neighbor.                                                              | This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor. |
| State                    | State of the RIP connection: <b>Up</b> or <b>Dn</b> (Down).                            | —                                                                                                                     |
| Source Address           | Local source address.                                                                  | This value is the configured address of the interface on which RIP is enabled.                                        |
| Destination Address      | Destination address.                                                                   | This value is the configured address of the immediate RIP adjacency.                                                  |
| Send Mode                | The mode of sending RIP messages.                                                      | —                                                                                                                     |
| Receive Mode             | The mode in which messages are received.                                               | —                                                                                                                     |
| In Metric                | Value of the incoming metric configured for the RIP neighbor.                          | —                                                                                                                     |

## Monitoring OSPF Routing Information

**Purpose** View OSPF routing information, including a summary of OSPF neighbors, interfaces, and statistics.

**Action** Select **Monitor>Routing>OSPF Information** in the J-Web user interface, or enter the following CLI commands:

- **show ospf neighbors**

- **show ospf interfaces**
- **show ospf statistics**

Table 186 summarizes key output fields in the OSPF routing display in the J-Web user interface.

**Table 186: Summary of Key OSPF Routing Output Fields**

| Field                    | Values                                                                                                                            | Additional Information                                                                                                                                                                          |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OSPF Interfaces</b>   |                                                                                                                                   |                                                                                                                                                                                                 |
| Details                  | Tab used to view the details of the selected OSPF.                                                                                | —                                                                                                                                                                                               |
| Interface                | Name of the interface running OSPF.                                                                                               | —                                                                                                                                                                                               |
| State                    | State of the interface: <b>BDR</b> , <b>Down</b> , <b>DR</b> , <b>DROther</b> , <b>Loop</b> , <b>PtToPt</b> , or <b>Waiting</b> . | The <b>Down</b> state, indicating that the interface is not functioning, and <b>PtToPt</b> state, indicating that a point-to-point connection has been established, are the most common states. |
| Area                     | Number of the area that the interface is in.                                                                                      | —                                                                                                                                                                                               |
| DR ID                    | ID of the area's designated device.                                                                                               | —                                                                                                                                                                                               |
| BDR ID                   | ID of the area's backup designated device.                                                                                        | —                                                                                                                                                                                               |
| Neighbors                | Number of neighbors on this interface.                                                                                            | —                                                                                                                                                                                               |
| <b>OSPF Statistics</b>   |                                                                                                                                   |                                                                                                                                                                                                 |
| <b>Packets tab</b>       |                                                                                                                                   |                                                                                                                                                                                                 |
| Sent                     | Displays the total number of packets sent.                                                                                        | —                                                                                                                                                                                               |
| Received                 | Displays the total number of packets received.                                                                                    | —                                                                                                                                                                                               |
| <b>Details tab</b>       |                                                                                                                                   |                                                                                                                                                                                                 |
| Flood Queue Depth        | Number of entries in the extended queue.                                                                                          | —                                                                                                                                                                                               |
| Total Retransmits        | Number of retransmission entries enqueued.                                                                                        | —                                                                                                                                                                                               |
| Total Database Summaries | Total number of database description packets.                                                                                     | —                                                                                                                                                                                               |
| <b>OSPF Neighbors</b>    |                                                                                                                                   |                                                                                                                                                                                                 |
| Address                  | Address of the neighbor.                                                                                                          | —                                                                                                                                                                                               |
| Interface                | Interface through which the neighbor is reachable.                                                                                | —                                                                                                                                                                                               |



Table 186: Summary of Key OSPF Routing Output Fields (*continued*)

| Field         | Values                                                                                                                                                 | Additional Information                                                                                                                                                                                                                                                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| State         | State of the neighbor: <b>Attempt</b> , <b>Down</b> , <b>Exchange</b> , <b>ExStart</b> , <b>Full</b> , <b>Init</b> , <b>Loading</b> , or <b>2way</b> . | Generally, only the <b>Down</b> state, indicating a failed OSPF adjacency, and the <b>Full</b> state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established. |
| ID            | ID of the neighbor.                                                                                                                                    | –                                                                                                                                                                                                                                                                                                              |
| Priority      | Priority of the neighbor to become the designated router.                                                                                              | –                                                                                                                                                                                                                                                                                                              |
| Activity Time | The activity time.                                                                                                                                     | –                                                                                                                                                                                                                                                                                                              |
| Area          | Area that the neighbor is in.                                                                                                                          | –                                                                                                                                                                                                                                                                                                              |
| Options       | Option bits received in the hello packets from the neighbor.                                                                                           | –                                                                                                                                                                                                                                                                                                              |
| DR Address    | Address of the designated router.                                                                                                                      | –                                                                                                                                                                                                                                                                                                              |
| BDR Address   | Address of the backup designated router.                                                                                                               | –                                                                                                                                                                                                                                                                                                              |
| Uptime        | Length of time since the neighbor came up.                                                                                                             | –                                                                                                                                                                                                                                                                                                              |
| Adjacency     | Length of time since the adjacency with the neighbor was established.                                                                                  | –                                                                                                                                                                                                                                                                                                              |

## Monitoring BGP Routing Information

**Purpose** Monitor BGP routing information on the routing device, including a summary of BGP routing and neighbor information.

**Action** Select **Monitor>Routing>BGP Information** in the J-Web user interface, or enter the following CLI commands:

- **show bgp summary**
- **show bgp neighbor**

[Table 187](#) summarizes key output fields in the BGP routing display in the J-Web user interface.

Table 187: Summary of Key BGP Routing Output Fields

| Field            | Values | Additional Information |
|------------------|--------|------------------------|
| BGP Peer Summary |        |                        |

Table 187: Summary of Key BGP Routing Output Fields (*continued*)

| Field                  | Values                                                                                                                                                                 | Additional Information |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Total Groups           | Number of BGP groups.                                                                                                                                                  | —                      |
| Total Peers            | Number of BGP peers.                                                                                                                                                   | —                      |
| Down Peers             | Number of unavailable BGP peers.                                                                                                                                       | —                      |
| Unconfigured Peers     | Address of each BGP peer.                                                                                                                                              | —                      |
| <b>RIB Summary tab</b> |                                                                                                                                                                        |                        |
| RIB Name               | Name of the RIB group.                                                                                                                                                 | —                      |
| Total Prefixes         | Total number of prefixes from the peer, both active and inactive, that are in the routing table.                                                                       | —                      |
| Active Prefixes        | Number of prefixes received from the EBGp peers that are active in the routing table.                                                                                  | —                      |
| Suppressed Prefixes    | Number of routes received from EBGp peers currently inactive because of damping or other reasons.                                                                      | —                      |
| History Prefixes       | History of the routes received or suppressed.                                                                                                                          | —                      |
| Dumped Prefixes        | Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols. | —                      |
| Pending Prefixes       | Number of pending routes.                                                                                                                                              | —                      |
| State                  | Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.  | —                      |
| <b>BGP Neighbors</b>   |                                                                                                                                                                        |                        |
| Details                | Click this button to view the selected BGP neighbor details.                                                                                                           | —                      |
| Peer Address           | Address of the BGP neighbor.                                                                                                                                           | —                      |
| Autonomous System      | AS number of the peer.                                                                                                                                                 | —                      |

Table 187: Summary of Key BGP Routing Output Fields (*continued*)

| Field        | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Additional Information                                                                                                                                                                                                                                                                                            |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Peer State   | <p>Current state of the BGP session:</p> <ul style="list-style-type: none"> <li>• <b>Active</b>—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message.</li> <li>• <b>Connect</b>—BGP is waiting for the TCP connection to become complete.</li> <li>• <b>Established</b>—The BGP session has been established, and the peers are exchanging BGP update messages.</li> <li>• <b>Idle</b>—This is the first stage of a connection. BGP is waiting for a Start event.</li> <li>• <b>OpenConfirm</b>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</li> <li>• <b>OpenSent</b>—BGP has sent an open message and is waiting to receive an open message from the peer.</li> </ul> | Generally, the most common states are <b>Active</b> , which indicates a problem establishing the BGP connection, and <b>Established</b> , which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time. |
| Elapsed Time | Elapsed time since the peering session was last reset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | —                                                                                                                                                                                                                                                                                                                 |
| Description  | Description of the BGP session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —                                                                                                                                                                                                                                                                                                                 |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## Monitoring Security Events by Policy

**Purpose** Monitor security events by policy and display logged event details with the J-Web user interface.

**Action** 1. Select **Monitor>Events and Alarms>Security Events** in the J-Web user interface. The View Policy Log pane appears. [Table 188](#) describes the content of this pane.

Table 188: View Policy Log Fields

| Field               | Value                                                        |
|---------------------|--------------------------------------------------------------|
| Log file name       | Name of the event log files to search.                       |
| Policy name         | Name of the policy of the events to be retrieved.            |
| Source address      | Source address of the traffic that triggered the event.      |
| Destination address | Destination address of the traffic that triggered the event. |

Table 188: View Policy Log Fields (*continued*)

| Field                | Value                                                         |
|----------------------|---------------------------------------------------------------|
| Event type           | Type of event that was triggered by the traffic.              |
| Application          | Application of the traffic that triggered the event.          |
| Source port          | Source port of the traffic that triggered the event.          |
| Destination port     | Destination port of the traffic that triggered the event.     |
| Source zone          | Source zone of the traffic that triggered the event.          |
| Destination zone     | Destination zone of the traffic that triggered the event.     |
| Source NAT rule      | Source NAT rule of the traffic that triggered the event.      |
| Destination NAT rule | Destination NAT rule of the traffic that triggered the event. |
| Is global policy     | Specifies that the policy is a global policy.                 |

If your device is not configured to store session log files locally, the Create log configuration button is displayed in the lower-right portion of the View Policy Log pane.

- To store session log files locally, click **Create log configuration**.

If session logs are being sent to an external log collector (stream mode has been configured for log files), a message appears indicating that event mode must be configured to view policy logs.



**NOTE:** Reverting to event mode will discontinue event logging to the external log collector.

- To reset the **mode** option to **event**, enter the **set security log** command.

2. Enter one or more search fields in the View Policy Log pane and click **Search** to display events matching your criteria.

For example, enter the event type **Session Close** and the policy **pol1** to display event details from all Session Close logs that contain the specified policy. To reduce search results further, add more criteria about the particular event or group of events that you want displayed.

The Policy Events Detail pane displays information from each matching session log. [Table 189](#) describes the contents of this pane.

Table 189: Policy Events Detail Fields

| Field                   | Value                                                                   |
|-------------------------|-------------------------------------------------------------------------|
| Timestamp               | Time when the event occurred.                                           |
| Policy name             | Policy that triggered the event.                                        |
| Record type             | Type of event log providing the data.                                   |
| Source IP/Port          | Source address (and port, if applicable) of the event traffic.          |
| Destination IP/Port     | Destination address (and port, if applicable) of the event traffic.     |
| Service name            | Service name of the event traffic.                                      |
| NAT source IP/Port      | NAT source address (and port, if applicable) of the event traffic.      |
| NAT destination IP/Port | NAT destination address (and port, if applicable) of the event traffic. |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)
  - [Monitoring Alarms on page 1712](#)
  - [Monitoring Events on page 1845](#)

## Monitoring Security Features

This section contains the following topics:

- [Monitoring Policies on page 1829](#)
- [Checking Policies on page 1832](#)
- [Monitoring Screen Counters on page 1835](#)
- [Monitoring IDP Status on page 1837](#)
- [Monitoring Flow Gate Information on page 1838](#)
- [Monitoring Firewall Authentication Table on page 1839](#)
- [Monitoring Firewall Authentication History on page 1841](#)
- [Monitoring 802.1x on page 1843](#)

### Monitoring Policies

- Purpose** Display, sort, and review policy activity for every activated policy configured on the device. Policies are grouped by Zone Context (the from and to zones of the traffic) to control the volume of data displayed at one time. From the policy list, select a policy to display statistics and current network activity.

**Action** To review policy activity:

1. Select **Monitor>Security>Policy>Activities** in the J-Web user interface. The Security Policies Monitoring page appears and lists the policies from the first Zone Context. See [Table 190](#) for field descriptions.
2. Select the **Zone Context** of the policy you want to monitor, and click **Filter**. All policies within the zone context appear in match sequence.
3. Select a policy, and click **Clear Statistics** to set all counters to zero for the selected policy.

**Table 190: Security Policies Monitoring Output Fields**

| Field                  | Value                                                                                                                                                                                                                                                                               | Additional Information                                                                                                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zone Context (Total #) | Displays a list of all from and to zone combinations for the configured policies. The total number of active policies for each context is specified in the Total # field. By default, the policies from the first Zone Context are displayed.                                       | To display policies for a different context, select a zone context and click <b>Filter</b> . Both inactive and active policies appear for each context. However, the Total # field for a context specifies the number of active policies only. |
| Default Policy action  | Specifies the action to take for traffic that does not match any of the policies in the context: <ul style="list-style-type: none"> <li>• permit-all—Permit all traffic that does not match a policy.</li> <li>• deny-all—Deny all traffic that does not match a policy.</li> </ul> | —                                                                                                                                                                                                                                              |
| From Zone              | Displays the source zone to be used as match criteria for the policy.                                                                                                                                                                                                               | —                                                                                                                                                                                                                                              |
| To Zone                | Displays the destination zone to be used as match criteria for the policy.                                                                                                                                                                                                          | —                                                                                                                                                                                                                                              |
| Name                   | Displays the name of the policy.                                                                                                                                                                                                                                                    | —                                                                                                                                                                                                                                              |
| Source Address         | Displays the source addresses to be used as match criteria for the policy. Address sets are resolved to their individual names. (In this case, only the names are given, not the IP addresses).                                                                                     | —                                                                                                                                                                                                                                              |
| Destination Address    | Displays the destination addresses (or address sets) to be used as match criteria for the policy. Addresses are entered as specified in the destination zone's address book.                                                                                                        | —                                                                                                                                                                                                                                              |
| Source Identity        | Displays the name of the source identities set for the policy.                                                                                                                                                                                                                      | To display the value of the source identities, hover the mouse on this field. Unknown source identities are also displayed.                                                                                                                    |
| Application            | Displays the name of a predefined or custom application signature to be used as match criteria for the policy.                                                                                                                                                                      | —                                                                                                                                                                                                                                              |

Table 190: Security Policies Monitoring Output Fields (*continued*)

| Field                     | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Additional Information                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic App               | <p>Displays the dynamic application signatures to be used as match criteria if an application firewall rule set is configured for the policy.</p> <p>For a network firewall, a dynamic application is not defined.</p>                                                                                                                                                                                                                                                                                                   | <p>The rule set appears in two lines. The first line displays the configured dynamic application signatures in the rule set. The second line displays the default dynamic application signature.</p> <p>If more than two dynamic application signatures are specified for the rule set, hover over the output field to display the full list in a tooltip.</p> |
| Action                    | <p>Displays the action portion of the rule set if an application firewall rule set is configured for the policy.</p> <ul style="list-style-type: none"> <li>• permit—Permits access to the network services controlled by the policy. A green background signifies permission.</li> <li>• deny—Denies access to the network services controlled by the policy. A red background signifies denial.</li> </ul>                                                                                                             | <p>The action portion of the rule set appears in two lines. The first line identifies the action to be taken when the traffic matches a dynamic application signature. The second line displays the default action when traffic does not match a dynamic application signature.</p>                                                                            |
| NW Services               | <p>Displays the network services permitted or denied by the policy if an application firewall rule set is configured. Network services include:</p> <ul style="list-style-type: none"> <li>• gprs-gtp-profile—Specify a GPRS Tunneling Protocol profile name.</li> <li>• idp—Perform intrusion detection and prevention.</li> <li>• redirect-wx—Set WX redirection.</li> <li>• reverse-redirect-wx—Set WX reverse redirection.</li> <li>• uac-policy—Enable unified access control enforcement of the policy.</li> </ul> | —                                                                                                                                                                                                                                                                                                                                                              |
| Policy Hit Counters Graph | <p>Provides a representation of the value over time for a specified counter. The graph is blank if Policy Counters indicates no data. As a selected counter accumulates data, the graph is updated at each refresh interval.</p>                                                                                                                                                                                                                                                                                         | <p>To toggle a graph on and off, click the counter name below the graph.</p>                                                                                                                                                                                                                                                                                   |

Table 190: Security Policies Monitoring Output Fields (*continued*)

| Field           | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Additional Information                                                                                                                             |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Counters | <p>Lists statistical counters for the selected policy if Count is enabled. The following counters are available for each policy:</p> <ul style="list-style-type: none"> <li>• input-bytes</li> <li>• input-byte-rate</li> <li>• output-bytes</li> <li>• output-byte-rate</li> <li>• input-packets</li> <li>• input-packet-rate</li> <li>• output-packets</li> <li>• output-packet-rate</li> <li>• session-creations</li> <li>• session-creation-rate</li> <li>• active-sessions</li> </ul> | To graph or to remove a counter from the Policy Hit Counters Graph, toggle the counter name. The names of enabled counters appear below the graph. |

## Checking Policies

- Purpose** Enter match criteria and conduct a policy search. The search results include all policies that match the traffic criteria in the sequence in which they will be encountered.
- Because policy matches are listed in the sequence in which they would be encountered, you can determine whether a specific policy is being applied correctly or not. The first policy in the list is applied to all matching traffic. Policies listed after this one remain in the “shadow” of the first policy and are never encountered by this traffic.
- By manipulating the traffic criteria and policy sequence, you can tune policy application to suit your needs. During policy development, you can use this feature to establish the appropriate sequence of policies for optimum traffic matches. When troubleshooting, use this feature to determine if specific traffic is encountering the appropriate policy.
- Action**
1. Select **Monitor>Security>Policy>Shadow Policies** in the J-Web user interface. The Check Policies page appears. [Table 191](#) explains the content of this page.
  2. In the top pane, enter the From Zone and To Zone to supply the context for the search.
  3. Enter match criteria for the traffic, including the source address and port, the destination address and port, and the protocol of the traffic.
  4. Enter the number of matching policies to display.
  5. Click **Search** to find policies matching your criteria. The lower pane displays all policies matching the criteria up to the number of policies you specified.
    - The first policy will be applied to all traffic with this match criteria.



- Remaining policies will not be encountered by any traffic with this match criteria.
6. To manipulate the position and activation of a policy, select the policy and click the appropriate button:
- **Move**—Moves the selected policy up or down to position it at a more appropriate point in the search sequence.
  - **Move to**—Moves the selected policy by allowing you to drag and drop it to a different location on the same page.

Table 191: Check Policies Output

| Field                                   | Function                                                                                                            |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Check Policies Search Input Pane</b> |                                                                                                                     |
| From Zone                               | Name or ID of the source zone. If a From Zone is specified by name, the name is translated to its ID internally.    |
| To Zone                                 | Name or ID of the destination zone. If a To Zone is specified by name, the name is translated to its ID internally. |
| Source Address                          | Address of the source in IP notation.                                                                               |
| Source Port                             | Port number of the source.                                                                                          |
| Destination Address                     | Address of the destination in IP notation.                                                                          |
| Destination Port                        | Port number of the destination.                                                                                     |
| Source Identity                         | Name of the source identity.                                                                                        |

Table 191: Check Policies Output (*continued*)

| Field                      | Function                                                                                                                                                                                                                                              |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol                   | Name or equivalent value of the protocol to be matched.<br><br>ah—51<br>egp—8<br>esp—50<br>gre—47<br>icmp—1<br>igmp—2<br>igp—9<br>ipip—94<br>ipv6—41<br>ospf—89<br>pgm—113<br>pim—103<br>rdp—27<br>rsvp—46<br>sctp—132<br>tcp—6<br>udp—17<br>vrrp—112 |
| Result Count               | (Optional) Number of policies to display. Default value is 1. Maximum value is 16.                                                                                                                                                                    |
| <b>Check Policies List</b> |                                                                                                                                                                                                                                                       |
| From Zone                  | Name of the source zone.                                                                                                                                                                                                                              |
| To Zone                    | Name of the destination zone.                                                                                                                                                                                                                         |
| Total Policies             | Number of policies retrieved.                                                                                                                                                                                                                         |
| Default Policy action      | The action to be taken if no match occurs.                                                                                                                                                                                                            |
| Name                       | Policy name                                                                                                                                                                                                                                           |
| Source Address             | Name of the source address (not the IP address) of a policy. Address sets are resolved to their individual names.                                                                                                                                     |

Table 191: Check Policies Output (*continued*)

| Field               | Function                                                                                                                            |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Destination Address | Name of the destination address or address set. A packet's destination address must match this value for the policy to apply to it. |
| Source Identity     | Name of the source identity for the policy.                                                                                         |
| Application         | Name of a preconfigured or custom application of the policy match.                                                                  |
| Action              | Action taken when a match occurs as specified in the policy.                                                                        |
| Hit Counts          | Number of matches for this policy. This value is the same as the Policy Lookups in a policy statistics report.                      |
| Active Sessions     | Number of active sessions matching this policy.                                                                                     |

Alternatively, to list matching policies using the CLI, enter the **show security match-policies** command and include your match criteria and the number of matching policies to display.

## Monitoring Screen Counters

**Purpose** View screen statistics for a specified security zone.

**Action** Select **Monitor>Security>Screen Counters** in the J-Web user interface, or enter the following CLI command:

**show security screen statistics zone *zone-name***

Table 192 summarizes key output fields in the screen counters display.

Table 192: Summary of Key Screen Counters Output Fields

| Field        | Values                                                      | Additional Information                                                                                                                                                               |
|--------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Zones</b> |                                                             |                                                                                                                                                                                      |
| ICMP Flood   | Internet Control Message Protocol (ICMP) flood counter.     | An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.                                  |
| UDP Flood    | User Datagram Protocol (UDP) flood counter.                 | UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled. |
| TCP Winnuke  | Number of Transport Control Protocol (TCP) WinNuke attacks. | WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows.                                                                                  |

Table 192: Summary of Key Screen Counters Output Fields (*continued*)

| Field                  | Values                                                     | Additional Information                                                                                                                                     |
|------------------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP Port Scan          | Number of TCP port scans.                                  | The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target.       |
| ICMP Address Sweep     | Number of ICMP address sweeps.                             | An IP address sweep can occur with the intent of triggering responses from active hosts.                                                                   |
| IP Tear Drop           | Number of teardrop attacks.                                | Teardrop attacks exploit the reassembly of fragmented IP packets.                                                                                          |
| TCP SYN Attack         | Number of TCP SYN attacks.                                 | —                                                                                                                                                          |
| IP Spoofing            | Number of IP spoofs.                                       | IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.                |
| ICMP Ping of Death     | ICMP ping of death counter.                                | Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes).                                                         |
| IP Source Route        | Number of IP source route attacks.                         | —                                                                                                                                                          |
| TCP Land Attack        | Number of land attacks.                                    | Land attacks occur when attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.          |
| TCP SYN Fragment       | Number of TCP SYN fragments.                               | —                                                                                                                                                          |
| TCP No Flag            | Number of TCP headers without flags set.                   | A normal TCP segment header has at least one control flag set.                                                                                             |
| IP Unknown Protocol    | Number of unknown Internet protocols.                      | —                                                                                                                                                          |
| IP Bad Options         | Number of invalid options.                                 | —                                                                                                                                                          |
| IP Record Route Option | Number of packets with the IP record route option enabled. | This option records the IP addresses of the network devices along the path that the IP packet travels.                                                     |
| IP Timestamp Option    | Number of IP timestamp option attacks.                     | This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination. |
| IP Security Option     | Number of IP security option attacks.                      | —                                                                                                                                                          |

Table 192: Summary of Key Screen Counters Output Fields (*continued*)

| Field                         | Values                                                      | Additional Information                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Loose route Option         | Number of IP loose route option attacks.                    | This option specifies a partial route list for a packet to take on its journey from source to destination.                                                                                                                                                                         |
| IP Strict Source Route Option | Number of IP strict source route option attacks.            | This option specifies the complete route list for a packet to take on its journey from source to destination.                                                                                                                                                                      |
| IP Stream Option              | Number of stream option attacks.                            | This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams.                                                                                                                                                     |
| ICMP Fragment                 | Number of ICMP fragments.                                   | Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.                                                                                   |
| ICMP Large Packet             | Number of large ICMP packets.                               | —                                                                                                                                                                                                                                                                                  |
| TCP SYN FIN Packet            | Number of TCP SYN FIN packets.                              | —                                                                                                                                                                                                                                                                                  |
| TCP FIN without ACK           | Number of TCP FIN flags without the acknowledge (ACK) flag. | —                                                                                                                                                                                                                                                                                  |
| TCP SYN-ACK-ACK Proxy         | Number of TCP flags enabled with SYN-ACK-ACK.               | To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, Junos OS rejects further connection requests from that IP address. |
| IP Block Fragment             | Number of IP block fragments.                               | —                                                                                                                                                                                                                                                                                  |

## Monitoring IDP Status

**Purpose** View detailed information about the IDP Status, Memory, Counters, Policy Rulebase Statistics, and Attack table statistics.

**Action** To view Intrusion Detection and Prevention (IDP) table information, select **Monitor>Security>IDP>Status** in the J-Web user interface, or enter the following CLI commands:

- **show security idp status**
- **show security idp memory**

Table 193 summarizes key output fields in the IDP display.

Table 193: Summary of IDP Status Output Fields

| Field                            | Values                                                                                                | Additional Information |
|----------------------------------|-------------------------------------------------------------------------------------------------------|------------------------|
| <b>IDP Status</b>                |                                                                                                       |                        |
| Status of IDP                    | Displays the status of the current IDP policy.                                                        | —                      |
| Up Since                         | Displays the time from when the IDP policy first began running on the system.                         | —                      |
| Packets/Second                   | Displays the number of packets received and returned per second.                                      | —                      |
| Peak                             | Displays the maximum number of packets received per second and the time when the maximum was reached. | —                      |
| Kbits/Second                     | Displays the aggregated throughput (kilobits per second) for the system.                              | —                      |
| Peak Kbits                       | Displays the maximum kilobits per second and the time when the maximum was reached.                   | —                      |
| Latency (Microseconds)           | Displays the delay, in microseconds, for a packet to receive and return by a node .                   | —                      |
| Current Policy                   | Displays the name of the current installed IDP policy.                                                | —                      |
| <b>IDP Memory Status</b>         |                                                                                                       |                        |
| IDP Memory Statistics            | Displays the status of all IDP data plane memory.                                                     | —                      |
| PIC Name                         | Displays the name of the PIC.                                                                         | —                      |
| Total IDP Data Plane Memory (MB) | Displays the total memory space, in megabytes, allocated for the IDP data plane.                      | —                      |
| Used (MB)                        | Displays the used memory space, in megabytes, for the data plane.                                     | —                      |
| Available (MB)                   | Displays the available memory space, in megabytes, for the data plane.                                | —                      |

## Monitoring Flow Gate Information

- Purpose** View information about temporary openings known as pinholes or gates in the security firewall.
- Action** Select **Monitor>Security>Flow Gate** in the J-Web user interface, or enter the **show security flow gate** command.

Table 194 summarizes key output fields in the flow gate display.

**Table 194: Summary of Key Flow Gate Output Fields**

| Field                        | Values                                                                                                                                                                           | Additional Information |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <b>Flow Gate Information</b> |                                                                                                                                                                                  |                        |
| Hole                         | Range of flows permitted by the pinhole.                                                                                                                                         | —                      |
| Translated                   | Tuples used to create the session if it matches the pinhole: <ul style="list-style-type: none"> <li>• Source address and port</li> <li>• Destination address and port</li> </ul> | —                      |
| Protocol                     | Application protocol, such as UDP or TCP.                                                                                                                                        | —                      |
| Application                  | Name of the application.                                                                                                                                                         | —                      |
| Age                          | Idle timeout for the pinhole.                                                                                                                                                    | —                      |
| Flags                        | Internal debug flags for pinhole.                                                                                                                                                | —                      |
| Zone                         | Incoming zone.                                                                                                                                                                   | —                      |
| Reference count              | Number of resource manager references to the pinhole.                                                                                                                            | —                      |
| Resource                     | Resource manager information about the pinhole.                                                                                                                                  | —                      |

## Monitoring Firewall Authentication Table

**Purpose** View information about the authentication table, which divides firewall authentication user information into multiple parts.

**Action** Select **Monitor>Security>Firewall Authentication>Authentication Table** in the J-Web user interface. To view detailed information about the user with a particular identifier, select the ID on the Authentication Table page. To view detailed information about the user at a particular source IP address, select the Source IP on the Authentication Table page.

Alternatively, enter the following CLI **show** commands:

- **show security firewall-authentication users**
- **show security firewall-authentication users address *ip-address***
- **show security firewall-authentication users identifier *identifier***

Table 195 summarizes key output fields in firewall authentication table display.

Table 195: Summary of Key Firewall Authentication Table Output Fields

| Field                                             | Values                                                         | Additional Information |
|---------------------------------------------------|----------------------------------------------------------------|------------------------|
| <b>Firewall authentication users</b>              |                                                                |                        |
| Total users in table                              | Number of users in the authentication table.                   | —                      |
| <b>Authentication table</b>                       |                                                                |                        |
| ID                                                | Authentication identification number.                          | —                      |
| Source Ip                                         | IP address of the authentication source.                       | —                      |
| Age                                               | Idle timeout for the user.                                     | —                      |
| Status                                            | Status of authentication ( <b>success</b> or <b>failure</b> ). | —                      |
| user                                              | Name of the user.                                              | —                      |
| <b>Detailed report per ID selected: <i>ID</i></b> |                                                                |                        |
| Source Zone                                       | Name of the source zone.                                       | —                      |
| Destination Zone                                  | Name of the destination zone.                                  | —                      |
| profile                                           | Name of the profile.                                           | Users information.     |
| Authentication method                             | Path chosen for authentication.                                | —                      |
| Policy Id                                         | Policy Identifier.                                             | —                      |
| Interface name                                    | Name of the interface.                                         | —                      |
| Bytes sent by this user                           | Number of packets in bytes sent by this user.                  | —                      |
| Bytes received by this user                       | Number of packets in bytes received by this user.              | —                      |
| Client-groups                                     | Name of the client group.                                      | —                      |
| <b>Detailed report per Source Ip selected</b>     |                                                                |                        |
| Entries from Source IP                            | IP address of the authentication source.                       | —                      |
| Source Zone                                       | Name of the source zone.                                       | —                      |
| Destination Zone                                  | Name of the destination zone.                                  | —                      |
| profile                                           | Name of the profile.                                           | —                      |
| Age                                               | Idle timeout for the user.                                     | —                      |
| Status                                            | Status of authentication ( <b>success</b> or <b>failure</b> ). | —                      |



Table 195: Summary of Key Firewall Authentication Table Output Fields (*continued*)

| Field                       | Values                                            | Additional Information |
|-----------------------------|---------------------------------------------------|------------------------|
| user                        | Name of the user.                                 | —                      |
| Authentication method       | Path chosen for authentication.                   | —                      |
| Policy Id                   | Policy Identifier.                                | —                      |
| Interface name              | Name of the interface.                            | —                      |
| Bytes sent by this user     | Number of packets in bytes sent by this user.     | —                      |
| Bytes received by this user | Number of packets in bytes received by this user. | —                      |
| Client-groups               | Name of the client group.                         | —                      |

## Monitoring Firewall Authentication History

**Purpose** View information about the authentication history, which is divided into multiple parts.

**Action** Select **Monitor>Security>Firewall Authentication>Authentication History** in the J-Web user interface. To view the detailed history of the authentication with this identifier, select the ID on the Firewall Authentication History page. To view a detailed authentication history of this source IP address, select the Source IP on the Firewall Authentication History page.

Alternatively, enter the following CLI **show** commands:

- **show security firewall-authentication history**
- **show security firewall-authentication history address *ip-address***
- **show security firewall-authentication history identifier *identifier***

Table 196 summarizes key output fields in firewall authentication history display.

Table 196: Summary of Key Firewall Authentication History Output Fields

| Field                                          | Values                                   | Additional Information |
|------------------------------------------------|------------------------------------------|------------------------|
| <b>History of Firewall Authentication Data</b> |                                          |                        |
| Total authentications                          | Number of authentication.                | —                      |
| <b>History Table</b>                           |                                          |                        |
| ID                                             | Identification number.                   | —                      |
| Source Ip                                      | IP address of the authentication source. | —                      |

Table 196: Summary of Key Firewall Authentication History Output Fields (*continued*)

| Field                                                 | Values                                                         | Additional Information |
|-------------------------------------------------------|----------------------------------------------------------------|------------------------|
| Start Date                                            | Authentication date.                                           | —                      |
| Start Time                                            | Authentication time.                                           | —                      |
| Duration                                              | Authentication duration.                                       | —                      |
| Status                                                | Status of authentication ( <b>success</b> or <b>failure</b> ). | —                      |
| User                                                  | Name of the user.                                              | —                      |
| <b>Detail history of selected Id: ID</b>              |                                                                |                        |
| Authentication method                                 | Path chosen for authentication.                                | —                      |
| Policy Id                                             | Security policy identifier.                                    | —                      |
| Source zone                                           | Name of the source zone.                                       | —                      |
| Destination Zone                                      | Name of the destination zone.                                  | —                      |
| Interface name                                        | Name of the interface.                                         | —                      |
| Bytes sent by this user                               | Number of packets in bytes sent by this user.                  | —                      |
| Bytes received by this user                           | Number of packets in bytes received by this user.              | —                      |
| Client-groups                                         | Name of the client group.                                      | —                      |
| <b>Detail history of selected Source Ip:Source Ip</b> |                                                                |                        |
| User                                                  | Name of the user.                                              | —                      |
| Start Date                                            | Authentication date.                                           | —                      |
| Start Time                                            | Authentication time.                                           | —                      |
| Duration                                              | Authentication duration.                                       | —                      |
| Status                                                | Status of authentication ( <b>success</b> or <b>failure</b> ). | —                      |
| Profile                                               | Name of the profile.                                           | —                      |
| Authentication method                                 | Path chosen for authentication.                                | —                      |
| Policy Id                                             | Security policy identifier.                                    | —                      |
| Source zone                                           | Name of the source zone.                                       | —                      |

Table 196: Summary of Key Firewall Authentication History Output Fields (*continued*)

| Field                       | Values                                            | Additional Information |
|-----------------------------|---------------------------------------------------|------------------------|
| Destination Zone            | Name of the destination zone.                     | —                      |
| Interface name              | Name of the interface.                            | —                      |
| Bytes sent by this user     | Number of packets in bytes sent by this user.     | —                      |
| Bytes received by this user | Number of packets in bytes received by this user. | —                      |
| Client-groups               | Name of the client group.                         | —                      |

## Monitoring 802.1x

**Purpose** View information about 802.1X properties.

**Action** Select **Monitor>Security>802.1x** in the J-Web user interface, or enter the following CLI commands:

- **show dot1x interfaces *interface-name***
- **show dot1x authentication-failed-users**

[Table 197](#) summarizes the Dot1X output fields.

Table 197: Summary of Dot1X Output Fields

| Field                                      | Values                                                                  | Additional Information |
|--------------------------------------------|-------------------------------------------------------------------------|------------------------|
| Select Port                                | List of ports for selection.                                            | —                      |
| Number of connected hosts                  | Total number of hosts connected to the port.                            | —                      |
| Number of authentication bypassed hosts    | Total number of authentication-bypassed hosts with respect to the port. | —                      |
| <b>Authenticated Users Summary</b>         |                                                                         |                        |
| MAC Address                                | MAC address of the connected host.                                      | —                      |
| User Name                                  | Name of the user.                                                       | —                      |
| Status                                     | Information about the host connection status.                           | —                      |
| Authentication Due                         | Information about host authentication.                                  | —                      |
| <b>Authentication Failed Users Summary</b> |                                                                         |                        |

**Table 197: Summary of Dot1X Output Fields (*continued*)**

| Field       | Values                                         | Additional Information |
|-------------|------------------------------------------------|------------------------|
| MAC Address | MAC address of the authentication-failed host. | –                      |
| User Name   | Name of the authentication-failed user.        | –                      |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

# Monitoring Events, Services and System

- [Monitoring DHCP Client Bindings on page 1845](#)
- [Monitoring Events on page 1845](#)
- [Monitoring the System on page 1848](#)

## Monitoring DHCP Client Bindings

**Purpose** View information about DHCP client bindings.

**Action** Select **Monitor>Services>DHCP>Binding** in the J-Web user interface, or enter the **show system services dhcp binding** command.

[Table 198](#) summarizes the key output fields in the DHCP client binding displays.

**Table 198: Summary of Key DHCP Client Binding Output Fields**

| Field            | Values                                                                          | Additional Information |
|------------------|---------------------------------------------------------------------------------|------------------------|
| IP Address       | List of IP addresses the DHCP server has assigned to clients.                   | —                      |
| Hardware Address | Corresponding media access control (MAC) address of the client.                 | —                      |
| Type             | Type of binding assigned to the client: dynamic or static.                      | —                      |
| Lease Expires at | Date and time the lease expires, or <b>never</b> for leases that do not expire. | —                      |

- Related Documentation**
- [Monitoring PPPoE on page 1801](#)
  - [Understanding DHCP Client Operation](#)

## Monitoring Events

**Purpose** Use the monitoring functionality to view the events page.

**Action** To monitor events select **Monitor>Events and Alarms>View Events** in the J-Web user interface.



**NOTE:** When you use an HTTPS connection in the Microsoft Internet Explorer browser to save a report from this page in the J-Web interface, the error message "Internet Explorer was not able to open the Internet site" is displayed. This problem occurs because the Cache-Control: no cache HTTP header is added on the server side and Internet Explorer does not allow you to download the encrypted file with the Cache-Control: no cache HTTP header set in the response from the server.

As a workaround, refer to Microsoft Knowledge Base article 323308, which is available at this URL: <http://support.microsoft.com/kb/323308>. Also, you can alternatively use HTTP in the Internet Explorer browser or use HTTPS in the Mozilla Firefox browser to save a file from this page.

**Meaning** Table 199 summarizes key output fields in the events page.

**Table 199: Events Monitoring Page**

| Field                  | Value                                                                                      | Additional Information |
|------------------------|--------------------------------------------------------------------------------------------|------------------------|
| <b>Events Filter</b>   |                                                                                            |                        |
| System Log File        | Specifies the name of the system log file that records errors and events.                  | -                      |
| Process                | Specifies the system processes that generate the events to display.                        | -                      |
| Include archived files | Specifies to enable the option to include archived files.                                  | Select to enable.      |
| Date From              | Specifies the beginning date range to monitor. Set the date using the calendar pick tool.  | -                      |
| To                     | Specifies the end of the date range to monitor. Set the date using the calendar pick tool. | -                      |
| Event ID               | Specifies the specific ID of the error or event to monitor.                                | -                      |
| Description            | Enter a description for the errors or events.                                              | -                      |
| Search                 | Fetches the errors and events specified in the search criteria.                            | -                      |
| Reset                  | Clears the cache of errors and events that were previously selected.                       | -                      |

Table 199: Events Monitoring Page (*continued*)

| Field                | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Additional Information |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Generate Report      | Creates an HTML report based on the specified parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | -                      |
| <b>Events Detail</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                        |
| Process              | Displays the system process that generated the error or event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | -                      |
| Severity             | <p>Displays the severity level that indicates how seriously the triggering event affects routing platform functions. Only messages from the facility that are rated at that level or higher are logged. Possible severities and their corresponding color code are:</p> <ul style="list-style-type: none"> <li>• <b>Debug/Info/Notice (Green)</b>—Indicates conditions that are not errors but are of interest or might warrant special handling.</li> <li>• <b>Warning (Yellow)</b> — Indicates conditions that warrant monitoring.</li> <li>• <b>Error (Blue)</b> — Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.</li> <li>• <b>Critical (Pink)</b> — Indicates critical conditions, such as hard drive errors.</li> <li>• <b>Alert (Orange)</b> — Indicates conditions that require immediate correction, such as a corrupted system database.</li> <li>• <b>Emergency (Red)</b> — Indicates system panic or other conditions that cause the routing platform to stop functioning.</li> </ul> | -                      |
| Event ID             | Displays the unique ID of the error or event. The prefix on each code identifies the generating software process. The rest of the code indicates the specific event or error.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -                      |
| Event Description    | Displays a more detailed explanation of the message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -                      |
| Time                 | Time that the error or event occurred.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | -                      |

- Related Documentation**
- [Monitoring Alarms on page 1712](#)
  - [Monitoring Security Events by Policy on page 1827](#)

## Monitoring the System

---

The J-Web user interface lets you monitor a device's physical characteristics, current processing status and alarms, and ongoing resource utilization to quickly assess the condition of a device at any time.

On SRX Series devices, the **Dashboard** lets you customize your view by selecting which informational panes to include on the Dashboard.

This section contains the following topics:

- [Monitoring System Properties for SRX Series Devices on page 1848](#)
- [Monitoring Chassis Information on page 1850](#)
- [System Health Management for Branch SRX Series Devices on page 1852](#)

### Monitoring System Properties for SRX Series Devices

**Purpose** View system properties and customize the Dashboard.

When you start the J-Web user interface on an SRX Series device, the interface opens to the Dashboard. At the top and bottom of the page, the Dashboard displays an interactive representation of your device and a current log messages pane. By default, the center panes of the Dashboard display System Information, Resource Utilization, Security Resources, and System Alarms. However, you can customize the Dashboard panes to provide the best overview of your system.

**Action** To control the content and appearance of the Dashboard:

1. Click the **Preferences** icon at the top-right corner of the page. The Dashboard Preference dialog box appears.
2. Select the types of information you want to display.
3. (Optional) Specify the Automatically Refresh Data option to specify how often you want the data on the Dashboard to be refreshed.
4. Click **OK** to save the configuration or **Cancel** to clear it.
5. On the Dashboard, minimize, maximize, or drag the individual information panes to customize the display as needed.

Chassis View—Displays an image of the device chassis, including line cards, link states, errors, individual PICs, FPCs, fans, and power supplies.

You can use the Chassis View to link to corresponding configuration and monitoring pages for the device. To link to interface configuration pages for a selected port from the Chassis View, right-click the port in the device image and choose one of the following options:

- Chassis Information—Links to the Chassis page.
- Configure Port: *Port-name*—Links to the interfaces configuration page for the selected port.



- Monitor Port: *Port-name*—Links to the monitor interfaces page for the selected port.

System Identification—Displays the device's serial number, hostname, current software version, the BIOS version, the amount of time since the device was last booted, and the system's time.



NOTE:

- To view the BIOS version under system identification, delete your browser cookies.
- The hostname that appears in this pane is defined using the `set system hostname` command.

On SRX Series devices, security logs were always timestamped using the UTC time zone by running `set system time-zone utc` and `set security log utc-timestamp` CLI commands. Now, time zone can be defined using the local time zone by running the `set system time-zone time-zone` command to specify the local time zone that the system should use when timestamping the security logs.

Resource Utilization—Provides a graphic representation of resource use. Each bar represents the percentage of CPU, memory, or storage utilization for the data plane or the control plane.

Security Resources—Provides the maximum, configured, and active sessions; firewall and VPN policies; and IPsec VPNs. Click **Sessions**, **FW/VPN Policies**, or **IPsec VPNs** for detailed statistics about each category.

System Alarms—Indicates a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified.

File Usage—Displays the usage statistics for log files, temporary files, crash (core) files, and database files.

Login Sessions—Provides a list of all currently logged in sessions. The display includes user credentials, login time, and idle time for each session.

Chassis Status—Provides a snapshot of the current physical condition of the device, including temperature and fan status.

Storage Usage—Displays the storage usage report in detail.

Threat Activity—Provides information about the most current threats received on the device.

Message Logs—Displays log messages and errors. You can clear old logs from the Message Logs pane by clicking the Clear button.

To control the information that is displayed in the Chassis View, use the following options:

- To view an image of the front of the device, right-click the image and choose **View Front**.
- To view an image of the back of the device, right-click the image and choose **View Rear**.
- To enlarge or shrink the device view, use the **Zoom** bar.
- To return the device image to its original position and size, click **Reset**.



**NOTE:** To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View appears by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box. Clearing cookies in Internet Explorer also causes the Chassis View appear on the Dashboard page.

To return to the Dashboard at any time, select **Dashboard** in the J-Web user interface.

Alternatively, you can view system properties by entering the following **show** commands in the CLI:

- **show system uptime**
- **show system users**
- **show system storage**
- **show version**
- **show chassis hardware**

## Monitoring Chassis Information

**Purpose** View chassis properties, which include the status of hardware components on the device.

**Action** To view these chassis properties, select **Monitor>System View>Chassis Information** in the J-Web user interface.



**CAUTION:** Do not install a combination of Physical Interface Modules (PIMs) in a single chassis that exceeds the maximum power and heat capacity of the chassis. If power management is enabled, PIMs that exceed the maximum power and heat limits remain offline when the chassis is powered on. To check PIM power and heat status, use the **show chassis fpc** and **show chassis power-ratings** commands.

The Chassis Information page displays the following types of information:

- **Routing Engine Details**—This section of the page includes the following tabs:
  - **Master**—Master tab displays information about the routing engine, including the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.
  - **Backup**—If a backup routing engine is available, the Backup tab displays the routing engine module, model number, version, part number, serial number, memory utilization, temperature, and start time. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.



**NOTE:** If you need to contact customer support about the device chassis, supply them with the version and serial number displayed in the Routing Engine Details section of the page.

- **Power and Fan Tray Details**—This Details section of the page includes the following tabs:
  - **Power**—Power tab displays the names of the device's power supply units and their statuses.
  - **Fan**—Fan tab displays the names of the device's fans and their speeds (normal or high). (The fan speeds are adjusted automatically according to the current temperature.)
- **Chassis Component Details**—This section of the page includes the following tabs:
  - **General**—General tab displays the version number, part number, serial number, and description of the selected device component.
  - **Temperature**—Temperature tab displays the temperature of the selected device component (if applicable).
  - **Resource**—Resource tab displays the state, total CPU DRAM, and start time of the selected device component (if applicable).



**NOTE:** On some devices, you can have an FPC state as “offline.” You might want to put an FPC offline because of an error or if the FPC is not responding. You can put the FPC offline by using the CLI command `request chassis fpc slot number offline`.

- **Sub-Component**—Sub-Component tab displays information about the device's sub-components (if applicable). Details include the sub-component's version, part number, serial number, and description.

To control which component details appear, select a hardware component from the **Select component** list.

Alternatively, you can view chassis details by entering the following **show** commands in the CLI configuration editor:

- **show chassis hardware**
- **show chassis routing-engine**
- **show chassis environment**
- **show chassis redundant-power-supply**
- **show redundant-power-supply status**

## System Health Management for Branch SRX Series Devices

**Purpose** Tracking the utilization of critical resources in the system ensures that all parameters are within normal limits and the system remains functional.

In the event of a malfunction caused by abnormal resource usage, the system health management feature provides the right diagnostic information to identify the source of the problem.

When the system health management action is configured by the user, the system takes appropriate monitoring, preventive, and recovery actions to ensure that the system is accessible. The system configuration might be updated based on the information collected by system health management feature to ensure that the system stays in the normal operating environment. For example, when a system runs out of memory, then the configuration associated with applications identified to be consuming memory resources can be updated to bring down the memory resource consumption.

**Action** The system health management feature periodically monitors critical system resources against configurable thresholds. The resources that can be monitored include CPU usage, memory, storage, open-file-descriptor, process-count, and temperature. The system health management feature collects usage information for each resource at the configured interval and compares it against the three levels of thresholds: moderate, high, and critical. Based on the configurations, appropriate action is taken.

The intervals, thresholds, and action are associated with system health management and can be configured at both the resource level and the global level. Configurable and default levels are as follows:

- **Default configuration level**—Default configuration is applied when system health monitoring is enabled, and neither a global nor a resource-specific configuration is present.
- **Global configuration level**—Configuration that is applied to resources when no resource-specific configuration is available.
- **Resource-specific configuration level**—Configuration that, if available, overrides both the global and the default configurations.

Per-resource configurations take precedence over the global configuration, and a global configuration takes precedence over the defaults.

When resource usage exceeds the configured thresholds, the system collects information that can be used to find the source of the increased usage and saves it in history for analysis and action.

When resource utilization exceeds the high threshold, a minor system alarm is generated, and the alarm LED lights yellow. When resource utilization exceeds the critical threshold, a major alarm is generated, and the alarm LED lights red.

An SNMP trap is also sent to the remote monitoring server (NMS) for all events that exceed the threshold.

To enable the system health monitor, use the **set snmp health-monitor routing engine** command. You can view system properties by using CLI show commands.

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)



# Monitoring Unified Threat Management Features

- [Monitoring Antivirus Scan Engine Status on page 1855](#)
- [Monitoring Antivirus Scan Results on page 1856](#)
- [Monitoring Antivirus Session Status on page 1858](#)
- [Monitoring Content Filtering Configurations on page 1858](#)
- [Monitoring Reports on page 1859](#)
- [Monitoring Web Filtering Configurations on page 1866](#)

## Monitoring Antivirus Scan Engine Status

---

**Purpose** Using the CLI, you can view the following scan engine status items:

Antivirus license key status

- View license expiration dates.

Scan engine status and settings

- View last action result.
- View default file extension list.

Antivirus pattern update server settings

- View update URL (HTTP or HTTPS-based).
- View update interval.

Antivirus pattern database status

- View auto update status.
- View last result of database loading.
- If the download completes, view database version timestamp virus record number.
- If the download fails, view failure reason.

**Action** In the CLI, enter the `user@host> show security utm anti-virus status` command.

Example status result:

```
AV Key Expire Date: 03/01/2010 00:00:00
Update Server: http://update.juniper-updates.net/AV/device-name
interval: 60 minutes
auto update status: next update in 12 minutes
last result: new database loaded
AV signature version: 12/21/2008 00:35 GMT, virus records: 154018
Scan Engine Info: last action result: No error(0x00000000)
```

- Related Documentation**
- *Full Antivirus Configuration Overview*
  - [Monitoring Antivirus Session Status on page 1858](#)
  - [Monitoring Antivirus Scan Results on page 1856](#)

---

## Monitoring Antivirus Scan Results

---

**Purpose** View statistics for antivirus requests, scan results, and fallback counters.

Scan requests provide

- The total number of scan request forwarded to the engine.
- The number of scan request being pre-windowed.
- The number of scan requests using scan-all mode.
- The number of scan requests using scan-by-extension mode.

Scan code counters provide

- Number of clean files.
- Number of infected files.
- Number of password protected files.
- Number of decompress layers.
- Number of corrupt files.
- When the engine is out of resources.
- When there is an internal error.

Fallback applied status provides either a log-and-permit or block result when the following has occurred

- Scan engine not ready.
- Maximum content size reached.
- Too many requests.
- Password protected file found.
- Decompress layer too large.
- Corrupt file found.



- Timeout occurred.
- Out of resources.
- Other.

**Action** To view antivirus scan results using the CLI editor, enter the **user@host> show security utm anti-virus statistics status** command.

To view antivirus scan results using J-Web:

1. Select **Monitor>Security>UTM>Anti-Virus**.

The following information becomes viewable in the right pane.

Antivirus license key status

- View license expiration dates.

Antivirus pattern update server settings

- View update URL (HTTP or HTTPS-based).
- View update interval.

Antivirus pattern database status

- View auto update status.
- View last result of database loading.
- If the download completes, view database version timestamp virus record number.
- If the download fails, view failure reason.

Antivirus statistics provide

- The number of scan request being pre-windowed.
- The total number of scan request forwarded to the engine.
- The number of scan requests using scan-all mode.
- The number of scan requests using scan-by-extension mode.

Scan code counters provide

- Number of clean files.
- Number of infected files.
- Number of password protected files.
- Number of decompress layers.
- Number of corrupt files.
- When the engine is out of resources.
- When there is an internal error.

Fallback applied status provides either a log-and-permit or block result when the following has occurred

- Scan engine not ready.
  - Password protected file found.
  - Decompress layer too large.
  - Corrupt file found.
  - Out of resources.
  - Timeout occurred.
  - Maximum content size reached.
  - Too many requests.
  - Other.
2. You can click the **Clear Anti-Virus Statistics** button to clear all current viewable statistics and begin collecting new statistics.

**Related Documentation** • [Monitoring Antivirus Session Status on page 1858](#)

---

## Monitoring Antivirus Session Status

**Purpose** Using the CLI, you can view the following session status items:

Antivirus session status displays a snapshot of current antivirus sessions. It includes

- Maximum supported antivirus session numbers.
- Total allocated antivirus session numbers.
- Total freed antivirus session numbers.
- Current active antivirus session numbers.

**Action** In the CLI, enter the **user@host> show security utm session status** command.

**Related Documentation** • [Full Antivirus Configuration Overview](#)  
• [Monitoring Antivirus Scan Engine Status on page 1855](#)  
• [Monitoring Antivirus Scan Results on page 1856](#)

---

## Monitoring Content Filtering Configurations

**Purpose** View content filtering statistics.

**Action** To view content filtering statistics in the CLI, enter the **user@host > show security utm content-filtering statistics** command.

The content filtering **show statistics** command displays the following information:

```
Base on command list: # Blocked
Base on mime list: # Blocked
Base on extension list: # Blocked
ActiveX plugin: # Blocked
Java applet: # Blocked
EXE files: # Blocked
ZIP files: # Blocked
HTTP cookie: # Blocked
```

To view content filtering statistics using J-Web:

1. Select **Clear Content filtering statistics** **Monitor>Security>UTM>Content Filtering** **Monitor>Security>UTM>Content Filtering**.

The following statistics become viewable in the right pane.

```
Base on command list: # Passed # Blocked
Base on mime list: # Passed # Blocked
Base on extension list: # Passed # Blocked
ActiveX plugin: # Passed # Blocked
Java applet: # Passed # Blocked
EXE files: # Passed # Blocked
ZIP files: # Passed # Blocked
HTTP cookie: # Passed # Blocked
```

2. You can click **Clear Content filtering statistics** to clear all current viewable statistics and begin collecting new statistics.

#### Related Documentation

- [Content Filtering Overview](#)
- [Understanding Content Filtering Protocol Support](#)
- [Content Filtering Configuration Overview](#)
- [Example: Attaching Content Filtering UTM Policies to Security Policies](#)

## Monitoring Reports

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action. The J-Web reporting feature provides one- or two-page reports that are equivalent to a compilation of numerous log entries.

This section contains the following topics:

- [Threats Monitoring Report on page 1859](#)
- [Traffic Monitoring Report on page 1864](#)

### Threats Monitoring Report

**Purpose** Use the Threats Report to monitor general statistics and activity reports of current threats to the network. You can analyze logging data for threat type, source and destination

details, and threat frequency information. The report calculates, displays, and refreshes the statistics, providing graphic presentations of the current state of the network.

**Action** To view the Threats Report:

1. Click **Threats Report** in the bottom right of the Dashboard, or select **Monitor>Reports>Threats** in the J-Web user interface. The Threats Report appears.
2. Select one of the following tabs:
  - **Statistics** tab. See [Table 200](#) for a description of the page content.
  - **Activities** tab. See [Table 201](#) for a description of the page content.

**Table 200: Statistics Tab Output in the Threats Report**

| Field                                     | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General Statistics Pane</b>            |                                                                                                                                                                                                                                                                                                                                                                                                       |
| Threat Category                           | One of the following categories of threats: <ul style="list-style-type: none"> <li>• Traffic</li> <li>• IDP</li> <li>• Content Security               <ul style="list-style-type: none"> <li>• Antivirus</li> <li>• Antispam</li> <li>• Web Filter—Click the Web filter category to display counters for 39 subcategories.</li> <li>• Content Filter</li> </ul> </li> <li>• Firewall Event</li> </ul> |
| Severity                                  | Severity level of the threat: <ul style="list-style-type: none"> <li>• emerg</li> <li>• alert</li> <li>• crit</li> <li>• err</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• debug</li> </ul>                                                                                                                                                                                         |
| Hits in past 24 hours                     | Number of threats encountered per category in the past 24 hours.                                                                                                                                                                                                                                                                                                                                      |
| Hits in current hour                      | Number of threats encountered per category in the last hour.                                                                                                                                                                                                                                                                                                                                          |
| <b>Threat Counts in the Past 24 Hours</b> |                                                                                                                                                                                                                                                                                                                                                                                                       |
| By Severity                               | Graph representing the number of threats received each hour for the past 24 hours sorted by severity level.                                                                                                                                                                                                                                                                                           |
| By Category                               | Graph representing the number of threats received each hour for the past 24 hours sorted by category.                                                                                                                                                                                                                                                                                                 |

Table 200: Statistics Tab Output in the Threats Report (*continued*)

| Field                                | Description                                                                                                                                                                                                                                                                  |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X Axis                               | Twenty-four hour span with the current hour occupying the right-most column of the display. The graph shifts to the left every hour.                                                                                                                                         |
| Y Axis                               | Number of threats encountered. The axis automatically scales based on the number of threats encountered.                                                                                                                                                                     |
| <b>Most Recent Threats</b>           |                                                                                                                                                                                                                                                                              |
| Threat Name                          | Names of the most recent threats. Depending on the threat category, you can click the threat name to go to a scan engine site for a threat description.                                                                                                                      |
| Category                             | Category of each threat: <ul style="list-style-type: none"> <li>Traffic</li> <li>IDP</li> <li>Content Security <ul style="list-style-type: none"> <li>Antivirus</li> <li>Antispam</li> <li>Web Filter</li> <li>Content Filter</li> </ul> </li> <li>Firewall Event</li> </ul> |
| Source IP/Port                       | Source IP address (and port number, if applicable) of the threat.                                                                                                                                                                                                            |
| Destination IP/Port                  | Destination IP address (and port number, if applicable) of the threat.                                                                                                                                                                                                       |
| Protocol                             | Protocol name of the threat.                                                                                                                                                                                                                                                 |
| Description                          | Threat identification based on the category type: <ul style="list-style-type: none"> <li>Antivirus—URL</li> <li>Web filter—category</li> <li>Content filter—reason</li> <li>Antispam—sender e-mail</li> </ul>                                                                |
| Action                               | Action taken in response to the threat.                                                                                                                                                                                                                                      |
| Hit Time                             | Time the threat occurred.                                                                                                                                                                                                                                                    |
| <b>Threat Trend in past 24 hours</b> |                                                                                                                                                                                                                                                                              |

Table 200: Statistics Tab Output in the Threats Report (*continued*)

| Field                       | Description                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category                    | <p>Pie chart graphic representing comparative threat counts by category:</p> <ul style="list-style-type: none"> <li>• Traffic</li> <li>• IDP</li> <li>• Content Security <ul style="list-style-type: none"> <li>• Antivirus</li> <li>• Antispam</li> <li>• Web Filter</li> <li>• Content Filter</li> </ul> </li> <li>• Firewall Event</li> </ul> |
| Web Filter Counters Summary |                                                                                                                                                                                                                                                                                                                                                  |
| Category                    | Web filter count broken down by up to 39 subcategories. Clicking on the Web filter listing in the General Statistics pane opens the Web Filter Counters Summary pane.                                                                                                                                                                            |
| Hits in past 24 hours       | Number of threats per subcategory in the last 24 hours.                                                                                                                                                                                                                                                                                          |
| Hits in current hour        | Number of threats per subcategory in the last hour.                                                                                                                                                                                                                                                                                              |

Table 201: Activities Tab Output in the Threats Report

| Field                  | Function                                                                                                                                                                                                              |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Most Recent Virus Hits |                                                                                                                                                                                                                       |
| Threat Name            | Name of the virus threat. Viruses can be based on services, like Web, FTP, or e-mail, or based on severity level.                                                                                                     |
| Severity               | <p>Severity level of each threat:</p> <ul style="list-style-type: none"> <li>• emerg</li> <li>• alert</li> <li>• crit</li> <li>• err</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• debug</li> </ul> |
| Source IP/Port         | IP address (and port number, if applicable) of the source of the threat.                                                                                                                                              |
| Destination IP/Port    | IP address (and port number, if applicable) of the destination of the threat.                                                                                                                                         |
| Protocol               | Protocol name of the threat.                                                                                                                                                                                          |

Table 201: Activities Tab Output in the Threats Report (*continued*)

| Field                                  | Function                                                                                                                                                                                                              |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                            | Threat identification based on the category type: <ul style="list-style-type: none"> <li>• Antivirus—URL</li> <li>• Web filter—category</li> <li>• Content filter—reason</li> <li>• Antispam—sender e-mail</li> </ul> |
| Action                                 | Action taken in response to the threat.                                                                                                                                                                               |
| Last Hit Time                          | Last time the threat occurred.                                                                                                                                                                                        |
| <b>Most Recent Spam E-Mail Senders</b> |                                                                                                                                                                                                                       |
| From e-mail                            | E-mail address that was the source of the spam.                                                                                                                                                                       |
| Severity                               | Severity level of the threat: <ul style="list-style-type: none"> <li>• emerg</li> <li>• alert</li> <li>• crit</li> <li>• err</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• debug</li> </ul>         |
| Source IP                              | IP address of the source of the threat.                                                                                                                                                                               |
| Action                                 | Action taken in response to the threat.                                                                                                                                                                               |
| Last Send Time                         | Last time that the spam e-mail was sent.                                                                                                                                                                              |
| <b>Recently Blocked URL Requests</b>   |                                                                                                                                                                                                                       |
| URL                                    | URL request that was blocked.                                                                                                                                                                                         |
| Source IP/Port                         | IP address (and port number, if applicable) of the source.                                                                                                                                                            |
| Destination IP/Port                    | IP address (and port number, if applicable) of the destination.                                                                                                                                                       |
| Hits in current hour                   | Number of threats encountered in the last hour.                                                                                                                                                                       |
| <b>Most Recent IDP Attacks</b>         |                                                                                                                                                                                                                       |
| Attack                                 |                                                                                                                                                                                                                       |

Table 201: Activities Tab Output in the Threats Report (*continued*)

| Field               | Function                                                                                                                                                                                                 |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity            | Severity of each threat: <ul style="list-style-type: none"> <li>• emerg</li> <li>• alert</li> <li>• crit</li> <li>• err</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• debug</li> </ul> |
| Source IP/Port      | IP address (and port number, if applicable) of the source.                                                                                                                                               |
| Destination IP/Port | IP address (and port number, if applicable) of the destination.                                                                                                                                          |
| Protocol            | Protocol name of the threat.                                                                                                                                                                             |
| Action              | Action taken in response to the threat.                                                                                                                                                                  |
| Last Send Time      | Last time the IDP threat was sent.                                                                                                                                                                       |

## Traffic Monitoring Report

**Purpose** Monitor network traffic by reviewing reports of flow sessions over the past 24 hours. You can analyze logging data for connection statistics and session usage by a transport protocol.

**Action** To view network traffic in the past 24 hours, select **Monitor>Reports>Traffic** in the J-Web user interface. See [Table 202](#) for a description of the report.

Table 202: Traffic Report Output

| Field                                         | Description                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sessions in Past 24 Hours per Protocol</b> |                                                                                                                                                                                                                                        |
| Protocol Name                                 | Name of the protocol. To see hourly activity by protocol, click the protocol name and review the “Protocol activities chart” in the lower pane. <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul> |
| Total Session                                 | Total number of sessions for the protocol in the past 24 hours.                                                                                                                                                                        |
| Bytes In (KB)                                 | Total number of incoming bytes in KB.                                                                                                                                                                                                  |
| Bytes Out (KB)                                | Total number of outgoing bytes in KB.                                                                                                                                                                                                  |



Table 202: Traffic Report Output (*continued*)

| Field                                | Description                                                                                                                                                                                                                                     |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packets In                           | Total number of incoming packets.                                                                                                                                                                                                               |
| Packets Out                          | Total number of outgoing packets.                                                                                                                                                                                                               |
| <b>Most Recently Closed Sessions</b> |                                                                                                                                                                                                                                                 |
| Source IP/Port                       | Source IP address (and port number, if applicable) of the closed session.                                                                                                                                                                       |
| Destination IP/Port                  | Destination IP address (and port number, if applicable) of the closed session.                                                                                                                                                                  |
| Protocol                             | Protocol of the closed session. <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>                                                                                                                          |
| Bytes In (KB)                        | Total number of incoming bytes in KB.                                                                                                                                                                                                           |
| Bytes Out (KB)                       | Total number of outgoing bytes in KB.                                                                                                                                                                                                           |
| Packets In                           | Total number of incoming packets.                                                                                                                                                                                                               |
| Packets Out                          | Total number of outgoing packets.                                                                                                                                                                                                               |
| Timestamp                            | The time the session was closed.                                                                                                                                                                                                                |
| <b>Protocol Activities Chart</b>     |                                                                                                                                                                                                                                                 |
| Bytes In/Out                         | Graphic representation of traffic as incoming and outgoing bytes per hour. The byte count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.     |
| Packets In/Out                       | Graphic representation of traffic as incoming and outgoing packets per hour. The packet count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately. |
| Sessions                             | Graphic representation of traffic as the number of sessions per hour. The session count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.       |
| X Axis                               | One hour per column for 24 hours.                                                                                                                                                                                                               |
| Y Axis                               | Byte, packet, or session count.                                                                                                                                                                                                                 |
| <b>Protocol Session Chart</b>        |                                                                                                                                                                                                                                                 |
| Sessions by Protocol                 | Graphic representation of the traffic as the current session count per protocol. The protocols displayed are TCP, UDP, and ICMP.                                                                                                                |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

---

## Monitoring Web Filtering Configurations

---

**Purpose** View Web-filtering statistics.

**Action** To view Web-filtering statistics using the CLI, enter the following commands:

```
user@host> show security utm web-filtering status
user@host> show security utm web-filtering statistics
```

To view Web-filtering statistics using J-Web:

1. Select **Clear Web Filtering Statistics**.

The following information is displayed in the right pane.

```
Total Requests: #
White List Hit: #
Black List Hit: #
Queries to Server: #
Server Reply Permit: #
Server Reply Block: #
Custom Category Permit: #
Custom Category Block: #
Cache Hit Permit: #
Cache Hit Block: #
Web Filtering Session Total: #
Web Filtering Session Inuse: #
Fall Back: Log-and-Permit Block
Default # #
Timeout # #
Server-Connectivity # #
Too-Many-Requests # #
```

2. You can click the **Clear Web Filtering Statistics** button to clear all current viewable statistics and begin collecting new statistics.

- Related Documentation**
- [Web Filtering Overview](#)
  - [Understanding Integrated Web Filtering](#)
  - [Example: Configuring Local Web Filtering](#)

# Monitoring VPNs

- [Monitoring VPNs on page 1867](#)

## Monitoring VPNs

This section contains the following topics:

- [Monitoring IKE Gateway Information on page 1867](#)
- [Monitoring IPsec VPN—Phase I on page 1871](#)
- [Monitoring IPsec VPN—Phase II on page 1872](#)
- [Monitoring IPsec VPN Information on page 1873](#)

### Monitoring IKE Gateway Information

**Purpose** View information about IKE security associations (SAs).

**Action** Select **Monitor>IPSec VPN>IKE Gateway** in the J-Web user interface. To view detailed information for a particular SA, select the IKE SA index on the IKE gateway page.

Alternatively, enter the following CLI commands:

- **show security ike security-associations**
- **show security ike security-associations index *index-id* detail**

[Table 203](#) summarizes key output fields in the IKE gateway display.

Table 203: Summary of Key IKE SA Information Output Fields

| Field                     | Values                                                                     | Additional Information                                                                              |
|---------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| IKE Security Associations |                                                                            |                                                                                                     |
| IKE SA Index              | Index number of an SA.                                                     | This number is an internally generated number you can use to display information about a single SA. |
| Remote Address            | IP address of the destination peer with which the local peer communicates. | —                                                                                                   |

Table 203: Summary of Key IKE SA Information Output Fields (*continued*)

| Field                                      | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Additional Information                                                                                                                               |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| State                                      | State of the IKE security associations: <ul style="list-style-type: none"> <li>• <b>DOWN</b>—SA has not been negotiated with the peer.</li> <li>• <b>UP</b>—SA has been negotiated with the peer.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | —                                                                                                                                                    |
| Initiator cookie                           | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | —                                                                                                                                                    |
| Responder cookie                           | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |
| Mode                                       | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are: <ul style="list-style-type: none"> <li>• <b>Main</b>—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• <b>Aggressive</b>—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul> | —                                                                                                                                                    |
| <b>IKE Security Association (SA) Index</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                      |
| IKE Peer                                   | IP address of the destination peer with which the local peer communicates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | —                                                                                                                                                    |
| IKE SA Index                               | Index number of an SA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | This number is an internally generated number you can use to display information about a single SA.                                                  |
| Role                                       | Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                                                                                                                                                    |
| State                                      | State of the IKE security associations: <ul style="list-style-type: none"> <li>• <b>DOWN</b>—SA has not been negotiated with the peer.</li> <li>• <b>UP</b>—SA has been negotiated with the peer.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | —                                                                                                                                                    |

Table 203: Summary of Key IKE SA Information Output Fields (*continued*)

| Field                 | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Additional Information                                                                                                                               |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initiator cookie      | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | –                                                                                                                                                    |
| Responder cookie      | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |
| Exchange Type         | <p>Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:</p> <ul style="list-style-type: none"> <li>• <b>Main</b>—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• <b>Aggressive</b>—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul> | –                                                                                                                                                    |
| Authentication Method | Path chosen for authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | –                                                                                                                                                    |
| Local                 | Address of the local peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | –                                                                                                                                                    |
| Remote                | Address of the remote peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | –                                                                                                                                                    |
| Lifetime              | Number of seconds remaining until the IKE SA expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | –                                                                                                                                                    |

Table 203: Summary of Key IKE SA Information Output Fields (*continued*)

| Field                       | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Additional Information |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Algorithm                   | <p>IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication algorithm used. <ul style="list-style-type: none"> <li>• <b>sha1</b>—Secure Hash Algorithm 1 (SHA-1) authentication.</li> <li>• <b>md5</b>—MD5 authentication.</li> </ul> </li> <li>• <b>Encryption</b>—Type of encryption algorithm used. <ul style="list-style-type: none"> <li>• <b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption.</li> <li>• <b>aes-192-cbc</b>—Advanced Encryption Standard (AES) 192-bit encryption.</li> <li>• <b>aes-128-cbc</b>—Advanced Encryption Standard (AES) 128-bit encryption.</li> <li>• <b>3des-cbc</b>—3 Data Encryption Standard (DES) encryption.</li> <li>• <b>des-cbc</b>—Data Encryption Standard (DES) encryption.</li> <li>• <b>Pseudorandom function</b>—Cryptographically secure pseudorandom function family.</li> </ul> </li> </ul> | —                      |
| Traffic Statistics          | <p>Traffic statistics include the following:</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—The number of bytes presented for processing by the device.</li> <li>• <b>Output bytes</b>—The number of bytes actually processed by the device.</li> <li>• <b>Input packets</b>—The number of packets presented for processing by the device.</li> <li>• <b>Output packets</b>—The number of packets actually processed by the device.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | —                      |
| IPsec security associations | <ul style="list-style-type: none"> <li>• <b>number created</b>—The number of SAs created.</li> <li>• <b>number deleted</b>—The number of SAs deleted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | —                      |
| Role                        | Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | —                      |
| Message ID                  | Message identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | —                      |
| Local identity              | Specifies the identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as any of the following: IPv4 address, fully qualified domain name, e-mail address, or distinguished name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | —                      |

Table 203: Summary of Key IKE SA Information Output Fields (*continued*)

| Field           | Values                                        | Additional Information |
|-----------------|-----------------------------------------------|------------------------|
| Remote identity | IPv4 address of the destination peer gateway. | —                      |

## Monitoring IPsec VPN—Phase I

**Purpose** View IPsec VPN Phase I information.

**Action** Select **Monitor>IPSec VPN>Phase I** in the J-Web user interface.

Table 204 describes the available options for monitoring IPsec VPN-Phase I.

Table 204: IPsec VPN—Phase I Monitoring Page

| Field                     | Values                                                                                                                                                                                     | Additional Information                                                                                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| IKE SA Tab Options        |                                                                                                                                                                                            |                                                                                                                                                      |
| IKE Security Associations |                                                                                                                                                                                            |                                                                                                                                                      |
| SA Index                  | Index number of an SA.                                                                                                                                                                     | —                                                                                                                                                    |
| Remote Address            | IP address of the destination peer with which the local peer communicates.                                                                                                                 | —                                                                                                                                                    |
| State                     | State of the IKE security associations: <ul style="list-style-type: none"> <li>DOWN—SA has not been negotiated with the peer.</li> <li>UP—SA has been negotiated with the peer.</li> </ul> | —                                                                                                                                                    |
| Initiator Cookie          | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.                                                                                    | —                                                                                                                                                    |
| Responder Cookie          | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.                                                                | A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |

Table 204: IPsec VPN—Phase I Monitoring Page (*continued*)

| Field | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Information |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Mode  | <p>Negotiation method agreed upon by the two IPsec endpoints, or peers, used to exchange information. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:</p> <ul style="list-style-type: none"> <li>• Main—The exchange is done with six messages. This mode, or exchange type, encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.</li> <li>• Aggressive—The exchange is done with three messages. This mode, or exchange type, does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul> | —                      |

## Monitoring IPsec VPN—Phase II

**Purpose** View IPsec VPN Phase II information.

**Action** Select **Monitor>IPSec VPN>Phase II** in the J-Web user interface.

Table 205 describes the available options for monitoring IPsec VPN-Phase II.

Table 205: IPsec VPN—Phase II Monitoring Page

| Field                              | Values                                                                                                | Additional Information |
|------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------|
| <b>Statistics Tab Details</b>      |                                                                                                       |                        |
| By bytes                           | Provides total number of bytes encrypted and decrypted by the local system across the IPsec tunnel.   | —                      |
| By packets                         | Provides total number of packets encrypted and decrypted by the local system across the IPsec tunnel. | —                      |
| IPsec Statistics                   | Provides details of the IPsec statistics.                                                             | —                      |
| <b>IPsec SA Tab Details</b>        |                                                                                                       |                        |
| <b>IPsec Security Associations</b> |                                                                                                       |                        |
| ID                                 | Index number of the SA.                                                                               | —                      |
| Gateway/Port                       | IP address of the remote gateway/port.                                                                | —                      |



Table 205: IPsec VPN—Phase II Monitoring Page (*continued*)

| Field      | Values                                                                                                                                                                                                                                                                                                                                                                   | Additional Information |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Algorithm  | <p>Cryptography scheme used to secure exchanges between peers during the IKE Phase II negotiations:</p> <ul style="list-style-type: none"> <li>An authentication algorithm used to authenticate exchanges between the peers. Options are hmac-md5-95 or hmac-sha1-96.</li> </ul>                                                                                         | —                      |
| SPI        | <p>Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase I and Phase II.</p> | —                      |
| Life       | The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.                                                                                                                                                                                                                                                                                | —                      |
| Monitoring | Specifies if VPN-Liveliness Monitoring has been enabled/disabled. Enabled - 'U ', Disabled- '—'                                                                                                                                                                                                                                                                          | —                      |
| Vsys       | Specifies the root system.                                                                                                                                                                                                                                                                                                                                               | —                      |

## Monitoring IPsec VPN Information

**Purpose** View information about IPsec security (SAs).

**Action** Select **Monitor>IPSec VPN>IPsec VPN** in the J-Web user interface. To view the IPsec statistics information for a particular SA, select the IPsec SA ID value on the IPsec VPN page.

Alternatively, enter the following CLI commands:

- show security ipsec security-associations**
- show security ipsec statistics**

Table 206 summarizes key output fields in the IPsec VPN display.

Table 206: Summary of Key IPsec VPN Information Output Fields

| Field                       | Values | Additional Information |
|-----------------------------|--------|------------------------|
| IPsec Security Associations |        |                        |

Table 206: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field               | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Information                                                            |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Total configured SA | Total number of IPsec security associations (SAs) configured on the device.                                                                                                                                                                                                                                                                                                                                                                                       | —                                                                                 |
| ID                  | Index number of the SA.                                                                                                                                                                                                                                                                                                                                                                                                                                           | —                                                                                 |
| Gateway             | IP address of the remote gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                 | —                                                                                 |
| Port                | If Network Address Translation (NAT-T) is used, this value is 4500. Otherwise, it is the standard IKE port, 500.                                                                                                                                                                                                                                                                                                                                                  | —                                                                                 |
| Algorithm           | <p>Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations:</p> <ul style="list-style-type: none"> <li>An authentication algorithm used to authenticate exchanges between the peers. Options are <b>hmac-md5-95</b> or <b>hmac-sha1-96</b>.</li> <li>An encryption algorithm used to encrypt data traffic. Options are <b>3des-cbc</b>, <b>aes-128-cbc</b>, <b>aes-192-cbc</b>, <b>aes-256-cbc</b>, or <b>des-cbc</b>.</li> </ul> | —                                                                                 |
| SPI                 | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.                                                                                                  | —                                                                                 |
| Life: sec/kb        | The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.                                                                                                                                                                                                                                                                                                                                                                         | —                                                                                 |
| State               | <p>State has two options, <b>Installed</b> and <b>Not Installed</b>.</p> <ul style="list-style-type: none"> <li><b>Installed</b>—The security association is installed in the security association database.</li> <li><b>Not Installed</b>—The security association is not installed in the security association database.</li> </ul>                                                                                                                             | For <b>transport</b> mode, the value of <b>State</b> is always <b>Installed</b> . |
| Vsys                | The root system.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | —                                                                                 |

---

#### IPsec Statistics Information

---

Table 206: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field                                 | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Information |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| ESP Statistics                        | <p>Encapsulation Security Protocol (ESP) statistics include the following:</p> <ul style="list-style-type: none"> <li>• <b>Encrypted bytes</b>—Total number of bytes encrypted by the local system across the IPsec tunnel.</li> <li>• <b>Decrypted bytes</b>—Total number of bytes decrypted by the local system across the IPsec tunnel.</li> <li>• <b>Encrypted packets</b>—Total number of packets encrypted by the local system across the IPsec tunnel.</li> <li>• <b>Decrypted packets</b>—Total number of packets decrypted by the local system across the IPsec tunnel.</li> </ul>                                                                                                                                                                                                                                                                                                       | —                      |
| AH Statistics                         | <p>Authentication Header (AH) statistics include the following:</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—The number of bytes presented for processing by the device.</li> <li>• <b>Output bytes</b>—The number of bytes actually processed by the device.</li> <li>• <b>Input packets</b>—The number of packets presented for processing by the device.</li> <li>• <b>Output packets</b>—The number of packets actually processed by the device.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                | —                      |
| Errors                                | <p>Errors include the following</p> <ul style="list-style-type: none"> <li>• <b>AH authentication failures</b>—Total number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel.</li> <li>• <b>Replay errors</b>—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window.</li> <li>• <b>ESP authentication failures</b>—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets.</li> <li>• <b>ESP decryption failures</b>—Total number of ESP decryption errors.</li> <li>• <b>Bad headers</b>—Total number of invalid headers detected.</li> <li>• <b>Bad trailers</b>—Total number of invalid trailers detected.</li> </ul> | —                      |
| Details for IPsec SA Index: <i>ID</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                        |
| Virtual System                        | The root system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | —                      |

Table 206: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field           | Values                                                                                                                                                                                                                                                                                                                                                                                        | Additional Information |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Local Gateway   | Gateway address of the local system.                                                                                                                                                                                                                                                                                                                                                          | —                      |
| Remote Gateway  | Gateway address of the remote system.                                                                                                                                                                                                                                                                                                                                                         | —                      |
| Local identity  | Specifies the identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as any of the following: IPv4 address, fully qualified domain name, e-mail address, or distinguished name.                                                                                                                                                   | —                      |
| Remote identity | IPv4 address of the destination peer gateway.                                                                                                                                                                                                                                                                                                                                                 | —                      |
| Df bit          | State of the don't fragment bit— <b>set</b> or <b>cleared</b> .                                                                                                                                                                                                                                                                                                                               | —                      |
| Policy name     | Name of the applicable policy.                                                                                                                                                                                                                                                                                                                                                                | —                      |
| Direction       | Direction of the security association— <b>inbound</b> , or <b>outbound</b> .                                                                                                                                                                                                                                                                                                                  | —                      |
| SPI             | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.                              | —                      |
| Mode            | Mode of the security association. Mode can be transport or tunnel. <ul style="list-style-type: none"> <li>• <b>transport</b>—Protects host-to-host connections.</li> <li>• <b>tunnel</b>—Protects connections between security gateways.</li> </ul>                                                                                                                                           | —                      |
| Type            | Type of the security association, either <b>manual</b> or <b>dynamic</b> . <ul style="list-style-type: none"> <li>• <b>manual</b>—Security parameters require no negotiation. They are static and are configured by the user.</li> <li>• <b>dynamic</b>—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode.</li> </ul> | —                      |

Table 206: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field                     | Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Information                                                                                                                                                                                                                                        |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| State                     | <p><b>State</b> has two options, <b>Installed</b>, and <b>Not Installed</b>.</p> <ul style="list-style-type: none"> <li>• <b>Installed</b>—The security association is installed in the security association database.</li> <li>• <b>Not Installed</b>—The security association is not installed in the security association database.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                 | For <b>transport</b> mode, the value of <b>State</b> is always <b>Installed</b> .                                                                                                                                                                             |
| Protocol                  | <p>Protocol supported:</p> <ul style="list-style-type: none"> <li>• <b>Transport</b> mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH).</li> <li>• <b>Tunnel</b> mode supports ESP and AH. <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication used.</li> <li>• <b>Encryption</b>—Type of encryption used.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              | —                                                                                                                                                                                                                                                             |
| Authentication/Encryption | <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication algorithm used. <ul style="list-style-type: none"> <li>• <b>sha1</b>—Secure Hash Algorithm 1 (SHA-1) authentication.</li> <li>• <b>md5</b>—MD5 authentication.</li> </ul> </li> <li>• <b>Encryption</b>—Type of encryption algorithm used. <ul style="list-style-type: none"> <li>• <b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption.</li> <li>• <b>aes-192-cbc</b>—Advanced Encryption Standard (AES) 192-bit encryption.</li> <li>• <b>aes-128-cbc</b>—Advanced Encryption Standard (AES) 128-bit encryption.</li> <li>• <b>3des-cbc</b>—3 Data Encryption Standard (DES) encryption.</li> <li>• <b>des-cbc</b>—Data Encryption Standard (DES) encryption.</li> </ul> </li> </ul> | —                                                                                                                                                                                                                                                             |
| Soft Lifetime             | <p>The soft lifetime informs the IPsec key management system that the SA is about to expire.</p> <ul style="list-style-type: none"> <li>• <b>Expires in seconds</b>—Number of seconds left until the SA expires.</li> <li>• <b>Expires in kilobytes</b>—Number of kilobytes left until the SA expires.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Each lifetime of a security association has two display options, <b>hard</b> and <b>soft</b> , one of which must be present for a dynamic security association. This allows the key management system to negotiate a new SA before the hard lifetime expires. |
| Hard Lifetime             | <p>The hard lifetime specifies the lifetime of the SA.</p> <ul style="list-style-type: none"> <li>• <b>Expires in seconds</b>—Number of seconds left until the SA expires.</li> <li>• <b>Expires in kilobytes</b>—Number of kilobytes left until the SA expires.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —                                                                                                                                                                                                                                                             |

Table 206: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field               | Values                                                                                                                                            | Additional Information                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Anti Replay Service | State of the service that prevents packets from being replayed. It can be <b>Enabled</b> or <b>Disabled</b> .                                     | –                                                                                                              |
| Replay Window Size  | Configured size of the antireplay service window. It can be 32 or 64 packets. If the replay window size is 0, the antireplay service is disabled. | The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. |

- Related Documentation**
- [Monitoring Overview on page 1397](#)
  - [Monitoring Interfaces on page 1794](#)

## PART 23

# Resource Monitoring of Memory Regions and Types Using CLI and SNMP Queries

- [Effective Troubleshooting of System Performance With Resource Monitoring Methodology on page 1881](#)





# Effective Troubleshooting of System Performance With Resource Monitoring Methodology

- [Resource Monitoring Usage Computation Overview on page 1881](#)
- [Resource Monitoring Mechanism on MX Series Routers Overview on page 1884](#)
- [Diagnosing and Debugging System Performance By Configuring Memory Resource Usage Monitoring on MX Series Routers on page 1886](#)
- [Managed Objects for Ukernel Memory for a Packet Forwarding Engine in an FPC Slot on page 1888](#)
- [Managed Objects for Packet Forwarding Engine Memory Statistics Data on page 1889](#)
- [Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot on page 1889](#)
- [jnxPfeMemoryErrorsTable on page 1890](#)
- [pfeMemoryErrors on page 1890](#)

## Resource Monitoring Usage Computation Overview

---

You can configure the resource monitoring capability using both the configuration statements in the CLI and SNMP MIB queries. You can employ this utility to provision sufficient headroom (memory space limits that are set for the application or virtual router) for monitoring the health and operating efficiency of DPCs and MPCs. To configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers. You can also analyze and view the usage or consumption of memory for the jtree memory type and for contiguous pages, double words, and free memory pages. The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. As the allocation of more memory for routing tables or firewall filters might disrupt the forwarding operations of a Packet Forwarding Engine, the Junos OS CLI displays a warning to restart all affected FPCs when you commit a configuration that includes the memory-enhanced route statement.

The following sections describe the computation equations and the interpretation of the different memory regions for I-chip-based and Trio-based line cards:

## Resource Monitoring and Usage Computation For Trio-Based Line Cards

In Trio-based line cards, memory blocks for next-hop and firewall filters are allocated separately. Also, an expansion memory is present, which is used when the allocated memory for next-hop or firewall filter is fully consumed. Both next-hop and firewall filters can allocate memory from the expansion memory. The encapsulation memory region is specific to I-chip-based line cards and it is not applicable to Trio-based line cards. Therefore, for Trio-based line cards, the percentage of free memory space can be interpreted as follows:

$$\% \text{ Free (NH)} = (1 - (\text{Used NH memory} + \text{Used Expansion memory}) / (\text{Total NH memory} + \text{Total Expansion memory})) \times 100$$
$$\% \text{ Free (Firewall or Filter)} = (1 - (\text{Used FW memory} + \text{Used Expansion memory}) / (\text{Total FW memory} + \text{Total Expansion memory})) \times 100$$

Encapsulation memory is I-chip-specific and is not applicable for Trio-based line cards.

% Free (Encap memory) = Not applicable

## Resource Monitoring and Usage Computation For I-Chip-Based Line Cards

I-chip-based line cards contain 32 MB of static RAM (SRAM) memory associated with the route lookup block and 16 MB of SRAM memory associated with the output WAN block.

The route-lookup memory is a single pool of 32 MB memory that is divided into two segments of 16 MB each. In a standard configuration, segment 0 is used for NH and prefixes, and segment 1 is used for firewall or filter. This allocation can be modified by using the route-memory-enhanced option at the [edit chassis] hierarchy level. In a general configuration, NH application can be allocated memory from any of the two segments. Therefore, the percentage of free memory for NH is calculated on 32 MB memory. Currently, firewall applications are allotted memory only from segment 1. As a result, the percentage of free memory to be monitored for firewall starts from the available 16 MB memory in segment 1 only.

For I-chip-based line cards, the percentage of free memory space can be interpreted as follows:

$$\% \text{ Free (NH)} = (32 - (\text{Used NH memory} + \text{Used FW memory} + \text{Used Other application})) / 32 \times 100$$
$$\% \text{ Free (Firewall or Filter)} = (16 - (\text{Used NH memory} + \text{Used FW memory} + \text{Used Other application})) / 16 \times 100$$

The memory size for Output WAN (lwo) SRAM is 16 MB and stores the Layer 2 descriptors that contain the encapsulation information. This entity is a critical resource and needs to be monitored. This memory space is displayed in the output of the show command as "Encap mem". The percentage of free memory for the encapsulation region is calculated as follows:

$\% \text{ Free (Encapsulation memory)} = (16 - (\text{two memory used (L2 descriptors + other applications)})) / 16 \times 100$

The watermark level configured for next-hop memory is also effective for encapsulation memory. Therefore, if the percentage of free memory for encapsulation region falls below the configured watermark, logs are generated.

If the free memory percentage is lower than the free memory watermark of a specific memory type, the following error message is recorded in the syslog:

**“Resource Monitor: FPC <slot no> PFE <pfe inst> <“JNH memory” or “FW/ Filter memory”> is below set watermark <configured watermark>”.**

You can configure resource-monitoring tracing operations by using the **traceoptions** file **<filename> flag flag level level size bytes** statement at the **[edit system services resource-monitor]** hierarchy level. By default, messages are written to **/var/log/rsmonlog**. The error logs associated with socket communication failure (between the Routing Engine and the Packet Forwarding Engine) are useful in diagnosing the problems in the communication between the Routing Engine and the Packet Forwarding Engine.

From the Ukern perspective, MPC5E contains only one Packet Forwarding Engine instance. The **show chassis fabric plane** command output displays the state of fabric plane connections to the Packet Forwarding Engine. Because two Packet Forwarding Engines exist, you notice PFE-0 and PFE-1 in the output.

```
user@host# run show chassis fabric plane
Fabric management PLANE state
Plane 0
 Plane state: ACTIVE
 FPC 0
 PFE 0 :Links ok
 PFE 1 :Links ok
```

Because only one Packet Forwarding Engine instance for MPC5E exists, the output of the **show system resource-monitor fpc** command displays only one row corresponding to Packet Forwarding Engine instance 0.

```
user@host# run show system resource-monitor fpc
FPC Resource Usage Summary
```

```
Free Heap Mem Watermark : 20 %
Free NH Mem Watermark : 20 %
Free Filter Mem Watermark : 20 %
```

\* - Watermark reached

|        | Heap   |       | ENCAP mem | NH mem | FW     |
|--------|--------|-------|-----------|--------|--------|
| mem    |        |       |           |        |        |
| Slot # | % Free | PFE # | % Free    | % Free | % Free |
| 0      | 94     | 0     |           | NA     | 83     |
| 99     |        |       |           |        |        |

The configured watermark is retained across GRES and unified ISSU procedures.

Related •  
Documentation

## Resource Monitoring Mechanism on MX Series Routers Overview

---

Junos OS supports a resource monitoring capability using both the configuration statements in the CLI interface and SNMP MIB queries. You can employ this utility to provision sufficient headroom (memory space limits that are set for the application or virtual router) for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. When the memory utilization, either the ukernel memory or ASIC memory reaches a certain threshold, the system operations compromise on the health and traffic-handling stability of the line card and such a trade-off on the system performance can be detrimental for supporting live traffic and protocols. Besides the ability to configure a threshold to raise error logs when a specific threshold value of resources is exceeded, you can also monitor the threshold values and resource utilization using SNMP MIB queries. You can configure watermark or checkpoint values for the line card resources, such as ukern memory (heap), next-hop (NH) memory, and firewall or filter memory, to be uniform for both Trio-based and I-chip-based line cards. The NH memory watermark is applicable only for encapsulation memory (output WAN static RAM memory). Encapsulation memory is specific to I-chips and not applicable for Trio-based chips. When the configured watermark is exceeded, error logs are triggered. If the resource has been used above a certain threshold, warning system log messages are generated to notify about the threshold value having exceeded. Based on your network needs, you can then determine whether you want to terminate any existing subscribers and services to prevent the system from being overloaded and resulting in a breakdown. This feature gathers input from each of the line cards and transfers this statistical detail to the Routing Engine process using a well-known internal port. This information is scanned by the daemon on the Routine Engine and using the shared memory space built into the session database, warning messages are generated for exceeded threshold conditions.

The capability to configure resource monitoring is supported on the MX80, MX104 routers and on the following line cards on MX240, MX480, MX960, MX2010, and MX2020 routers:

- MX-MPC1-3D
- MX-MPC1-3D-Q
- MX-MPC2-3D
- MX-MPC2-3D-Q
- MX-MPC2-3D-EQ
- MPC-3D-16XGE-SFPP
- MPC3E
- MPC4E-3D-2CGE-8XGE
- MPC4E-3D-32XGE
- MPC5EQ-40G10G

- MPC5EQ-100G10G
- MPC5E-100G10G
- MPC5E-40G10G
- MX2K-MPC6E
- DPCE
- MS-DPC
- MX Series Flexible PIC Concentrators (MX-FPCs)

You can configure the following parameters at the **[edit system services]** hierarchy level to specify the high threshold value that is common for all the memory spaces or regions and the watermark values for the different memory blocks on DPCs and MPCs:

- High threshold value, exceeding which warnings or error logs are generated, for all the regions of memory, such as heap or ukernel, next-hop and encapsulation, and firewall filter memory, by using the **set resource-monitor high-threshold value** statement.
- Percentage of free memory space used for next-hops to be monitored with a watermark value by using the **set resource-monitor free-nh-memory-watermark percentage** statement.
- Percentage of free memory space used for ukernel or heap memory to be monitored with a watermark value by using the **set resource-monitor free-heap-memory-watermark percentage** statement.
- Percentage of free memory space used for firewall and filter memory to be monitored with a watermark value by using the **set resource-monitor free-filter-memory-watermark percentage** statement. This feature is enabled by default and you cannot disable it manually. The default value and the configured value of the watermark value for the percentage of free next-hop memory also applies to encapsulation memory.

The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are as follows:

- free-heap-memory-watermark—20
- free-nh-memory-watermark—20
- free-filter-memory-watermark—20

## Examining the Utilization of Memory Resource Regions Using show Commands

You can use the **show system resource-monitor fpc** command to monitor the utilization of memory resources on the Packet Forwarding Engines of an FPC. The filter memory denotes the filter counter memory used for firewall filter counters. The asterisk (\*) displayed next to each of the memory regions denotes the ones for which the configured threshold is being currently exceeded. Resource monitoring commands display the configured values of watermark for memories for different line card applications to be monitored. The displayed statistical metrics are based on the computation performed of the current memory utilization of the individual line cards. The ukern memory is generic across the different types of line cards and signifies the heap memory buffers. Because

a line card or an FPC in a particular slot can contain multiple Packet Forwarding Engine complexes, the memory utilized on the application-specific integrated circuits (ASICs) are specific to a particular PFE complex. Owing to different architecture models for different variants of line cards supported, the ASIC-specific memory (next-hop and firewall or filter memory) utilization percentage can be interpreted differently.

**Related** •  
**Documentation**

## Diagnosing and Debugging System Performance By Configuring Memory Resource Usage Monitoring on MX Series Routers

---

Junos OS supports a resource monitoring capability using both the configuration statements in the CLI interface and SNMP MIB queries. You can employ this utility to provision sufficient headroom (memory space limits that are set for the application or virtual router) for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. When the memory utilization, either the ukernel memory or ASIC memory reaches a certain threshold, the system operations compromise on the health and traffic-handling stability of the line card and such a trade-off on the system performance can be detrimental for supporting live traffic and protocols. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers,

To configure the properties of the memory resource-utilization functionality:

1. Specify that you want to configure the monitoring mechanism for utilization of different memory resource regions.

```
[edit]
user@host# edit system services resource-monitor
```

This feature is enabled by default and you cannot disable it manually.

2. Specify the high threshold value, exceeding which warnings or error logs are generated, for all the regions of memory, such as heap or ukernel, next-hop and encapsulation, and firewall filter memory.

```
[edit system services resource-monitor]
user@host# set high-threshold value
```

3. Specify the percentage of free memory space used for next-hops to be monitored with a watermark value.

```
[edit system services resource-monitor]
user@host# set free-nh-memory-watermark percentage
```

4. Specify the percentage of free memory space used for ukernel or heap memory to be monitored with a watermark value.

```
[edit system services resource-monitor]
user@host# set free-heap-memory- watermark percentage
```

5. Specify the percentage of free memory space used for firewall and filter memory to be monitored with a watermark value.

```
[edit system services resource-monitor]
```

```
user@host# set free-filter-memory-memory- watermark percentage
```

**NOTE:**

The default value and the configured value of the watermark value for the percentage of free next-hop memory also applies to encapsulation memory. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20 percent.

6. Disable the generation of error log messages when the utilization of memory resources exceeds the threshold or checkpoint levels. By default, messages are written to `/var/log/rsmonlog`.

```
[edit system services resource-monitor]
user@host# set no-logging
```

7. Define the resource category that you want to monitor and analyze for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers. The resource category includes detailed CPU utilization, session rate, and session count statistics. You use the resource category statistics to understand the extent to which new attack objects or applications affect performance.

```
[edit system services resource-monitor]
user@host# edit resource-category jtree
```



**NOTE:** The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. The Junos OS provides the memory-enhanced statement to reallocate the jtree memory for routes, firewall filters, and Layer 3 VPNs.

8. Configure the type of resource as contiguous pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is contiguous page in this case.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type contiguous-pages high-threshold percentage
user@host# set resource-type contiguous-pages low-threshold percentage
```

9. Configure the type of resource as free double words (dwords) for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is free dwords in this case.

```
[edit system services resource-monitor resource-category jtree]
```

```

user@host# set resource-type free-dwords high-threshold percentage
user@host# set resource-type free-dwords low-threshold percentage

```

10. Configure the type of resource as free memory pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. Specify the high and low threshold value, exceeding which warnings or error logs are generated, for the specified type or region of memory, which is free memory pages in this case.

```

[edit system services resource-monitor resource-category jtree]
user@host# set resource-type free-pages high-threshold percentage
user@host# set resource-type free-pages low-threshold percentage

```

11. View the utilization of memory resources on the Packet Forwarding Engines of an FPC by using the **show system resource-monitor fpc** command. The filter memory denotes the filter counter memory used for firewall filter counters. The asterisk (\*) displayed next to each of the memory regions denotes the ones for which the configured threshold is being currently exceeded.

```

user@host# run show system resource-monitor fpc
FPC Resource Usage Summary

```

```

Free Heap Mem Watermark : 20 %
Free NH Mem Watermark : 20 %
Free Filter Mem Watermark : 20 %

```

```
* - Watermark reached
```

| FW mem |        | Heap  |        | ENCAP mem |        | NH mem |  |
|--------|--------|-------|--------|-----------|--------|--------|--|
| Slot # | % Free | PFE # | % Free | % Free    | % Free | %      |  |
| Free   |        |       |        |           |        |        |  |
| 0      | 94     | 0     |        | NA        | 83     |        |  |
| 99     |        |       |        |           |        |        |  |

Related •  
Documentation

## Managed Objects for Ukernl Memory for a Packet Forwarding Engine in an FPC Slot

The **jnxPfeMemoryUkernTable**, whose object identifier is **{jnxPfeMemory 1}**, contains the **JnxPfeMemoryUkernEntry** that retrieves the global ukernel or heap memory statistics for the specified Packet Forwarding Engine slot. Each **JnxPfeMemoryUkernEntry**, whose object identifier is **{jnxPfeMemoryUkernTable 1}**, contains the objects listed in the following table. The **jnxPfeMemoryUkernEntry** denotes the memory utilization, such as the total available memory and the percentage of memory used.

Table 207: jnxPfeMemoryUkernTable

| Object                       | Object ID                | Description                                                                           |
|------------------------------|--------------------------|---------------------------------------------------------------------------------------|
| jnxPfeMemoryUkernFreePercent | jnxPfeMemoryUkernEntry 3 | Denotes the percentage of free Packet Forwarding Engine memory within the ukern heap. |



## Managed Objects for Packet Forwarding Engine Memory Statistics Data

The **jnxPfeMemory** table, whose object identifier is **{jnxPfeMib 2}** contains the objects listed in [Table 208](#)

**Table 208: jnxPfeMemory Table**

| Object                             | Object ID             | Description                                                                                                                                                                                                       |
|------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>jnxPfeMemoryUkernTable</b>      | <b>jnxPfeMemory 1</b> | Provides global ukern memory statistics for the specified Packet Forwarding Engine slot.                                                                                                                          |
| <b>jnxPfeMemoryForwardingTable</b> | <b>jnxPfeMemory 2</b> | Provides global next-hop (for Trio-based line cards) or Jtree (for I-chip-based line cards) memory utilization and firewall filter memory utilization statistics for the specified Packet Forwarding Engine slot. |

## Managed Objects for Next-Hop, Jtree, and Firewall Filter Memory for a Packet Forwarding Engine in an FPC Slot

The **jnxPfeMemoryForwardingTable**, whose object identifier is **{jnxPfeMemory 2}**, contains **JnxPfeMemoryForwardingEntry** that retrieves the next-hop memory for Trio-based line cards, jtree memory for I-chip-based line cards, and firewall or filter memory statistics for the specified Packet Forwarding Engine slot for both I-chip and Trio-based line cards. Each **jnxPfeMemoryForwardingEntry**, whose object identifier is **{jnxPfeMemoryForwardingTable 1}**, contains the objects listed in the following table.

The **jnxPfeMemoryForwardingEntry** represents the ASIC instance, ASIC memory used, and ASIC free memory. The jtree memory on all MX Series router Packet Forwarding Engines has two segments: one segment primarily stores routing tables and related information, and the other segment primarily stores firewall-filter-related information. As the allocation of more memory for routing tables or firewall filters might disrupt the forwarding operations of a Packet Forwarding Engine, the Junos OS CLI displays a warning to restart all affected FPCs when you commit a configuration that includes the memory-enhanced route statement. The configuration does not become effective until you restart the FPC or DPC (on MX Series routers).

**Table 209: jnxPfeMemoryForwardingTable**

| Object                                   | Object ID                            | Description                                                                          |
|------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------|
| <b>jnxPfeMemoryForwardingChipSlot</b>    | <b>jnxPfeMemoryForwardingEntry 1</b> | Indicates the ASIC instance number in the Packet Forwarding Engine complex.          |
| <b>jnxPfeMemoryType</b>                  | <b>jnxPfeMemoryForwardingEntry 2</b> | Indicates the Packet Forwarding Engine memory type, where nh = 1, fw = 2, encap = 3. |
| <b>jnxPfeMemoryForwardingPercentFree</b> | <b>jnxPfeMemoryForwardingEntry 3</b> | Indicates the percentage of memory free for each memory type.                        |

## jnxPfeMemoryErrorsTable

The Juniper Networks enterprise-specific Packet Forwarding Engine MIB, whose object ID is **{jnxPfeMibRoot 1}**, supports a new MIB table, **jnxPfeMemoryErrorsTable**, to display Packet Forwarding Engine memory error counters. The **jnxPfeMemoryErrorsTable**, whose object identifier is **jnxPfeNotification 3**, contains the **JnxPfeMemoryErrorsEntry**. Each **JnxPfeMemoryErrorsEntry**, whose object identifier is **{jnxPfeMemoryErrorsTable 1}**, contains the objects listed in the following table.

Table 210: jnxPfeMemoryErrorsTable

| Object             | Object ID                 | Description                                                    |
|--------------------|---------------------------|----------------------------------------------------------------|
| jnxPfeFpcSlot      | jnxPfeMemoryErrorsEntry 1 | Signifies the FPC slot number for this set of PFE notification |
| jnxPfeSlot         | jnxPfeMemoryErrorsEntry 2 | Signifies the PFE slot number for this set of errors           |
| jnxPfeParityErrors | jnxPfeMemoryErrorsEntry 3 | Signifies the parity error count                               |
| jnxPfeEccErrors    | jnxPfeMemoryErrorsEntry 4 | Signifies the error-checking code (ECC) error count            |

## pfeMemoryErrors

The **pfeMemoryErrorsNotificationPrefix**, whose object identifier is **{jnxPfeNotification 0}**, contains the **pfeMemoryErrors** attribute. The **pfeMemoryErrors** object, whose identifier is **{pfeMemoryErrorsNotificationPrefix 1}** contains the **jnxPfeParityErrors** and **jnxPfeEccErrors** objects.

Table 211: pfeMemoryErrors

| Object          | Object ID                           | Description                                                                                               |
|-----------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------|
| pfeMemoryErrors | pfeMemoryErrorsNotificationPrefix 1 | A pfeMemoryErrors notification is sent when the value of jnxPfeParityErrors or jnxPfeEccErrors increases. |

## PART 24

# Troubleshooting

- [Configuring Data Path Debugging and Trace Options on page 1893](#)
- [Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits on page 1909](#)
- [Using Packet Capture to Analyze Network Traffic on page 1927](#)
- [Troubleshooting Security Devices on page 1953](#)



## CHAPTER 88

# Configuring Data Path Debugging and Trace Options

- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1894](#)
- [Example: Configuring End-to-End Debugging on a High-End SRX Series Device on page 1895](#)
- [Understanding Security Debugging Using Trace Options on page 1899](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1899](#)
- [Displaying Log and Trace Files on page 1900](#)
- [Displaying Output for Security Trace Options on page 1901](#)
- [Displaying Multicast Trace Operations on page 1901](#)
- [Using the J-Web Traceroute Tool on page 1902](#)
- [J-Web Traceroute Results and Output Summary on page 1904](#)
- [Understanding Flow Debugging Using Trace Options on page 1905](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1905](#)
- [Displaying a List of Devices on page 1906](#)

## Understanding Data Path Debugging for SRX Series Devices

---

Data path debugging, or end-to-end debugging, support provides tracing and debugging at multiple processing units along the packet-processing path. The packet filter can be executed with minimal impact to the production system.

On a high-end SRX Series device, a packet goes through series of events involving different components from ingress to egress processing.

With the data path debugging feature, you can trace and debug (capture packets) at different data points along the processing path. The events available in the packet-processing path are: NP ingress, load-balancing thread (LBT), jexec, packet-ordering thread (POT), and NP egress. You can also enable flow module trace if the security flow trace flag for a certain module is set.

At each event, you can specify any of the four actions (count, packet dump, packet summary, and trace). Data path debugging provides filters to define what packets to

capture, and only the matched packets are traced. The packet filter can filter out packets based on logical interface, protocol, source IP address prefix, source port, destination IP address prefix, and destination port.

To enable end-to-end debugging, you must perform the following steps:

1. Define the capture file and specify the maximum capture size.
2. Define the packet filter to trace only a certain type of traffic based on the requirement.
3. Define the action profile specifying the location on the processing path from where to capture the packets (for example, LBT or NP ingress).
4. Enable the data path debugging.
5. Capture traffic.
6. Disable data path debugging.
7. View or analyze the report.



**NOTE:**

The packet-filtering behavior for the port and interface options is as follows:

- The packet filter traces both IPv4 and IPv6 traffic if only **port** is specified.
  - The packet filter traces IPv4, IPV6, and non-IP traffic if only **interface** is specified.
- 

**Related Documentation**

- [Understanding Security Debugging Using Trace Options on page 1899](#)
- [Understanding Flow Debugging Using Trace Options on page 1905](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1894](#)
- [Example: Configuring End-to-End Debugging on a High-End SRX Series Device on page 1895](#)

---

## Debugging the Data Path (CLI Procedure)

---

To configure the device for data path debugging:

1. Specify the following request command to set the data path debugging for the multiple processing units along the packet-processing path:

```
[edit]
user@host# set security datapath-debug
```

2. Specify the trace options for data path-debug using the following command:

```
[edit]
user@host# set security datapath-debug traceoptions
```

- Using the request security packet-filter command, you can set the packet filter to specify the related packets to perform data path-debug action. A maximum of four filters are supported at the same time. For example, the following command sets the first packet-filter:

```
[edit]
user@host# set security datapath-debug packet-filter name
```

- Using the request security action-profile command, you can set the action for the packet match for a specified filter. Only the default action profile is supported, which is the trace option for network processor ezchip ingress, ezchip egress, spu.lbt, and spu.pot:

```
[edit]
user@host# set security datapath-debug packet-filter name action-profile
```

#### Related Documentation

- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)
- [Understanding Security Debugging Using Trace Options on page 1899](#)
- [Understanding Flow Debugging Using Trace Options on page 1905](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1905](#)

## Example: Configuring End-to-End Debugging on a High-End SRX Series Device

This example shows how to configure end-to-end debugging on an SRX Series device with an SRX5K-MPC.

- [Requirements on page 1895](#)
- [Overview on page 1895](#)
- [Configuration on page 1896](#)
- [Enabling Data Path Debugging on page 1898](#)
- [Verification on page 1898](#)

### Requirements

This example uses the following hardware and software components:

- SRX5600 device with an SRX5K-MPC installed with 100-Gigabit Ethernet CFP installed
- Junos OS Release 12.1X47-D15 or later for SRX Series devices

Before you begin:

- See *Understanding Data Path Debugging for SRX Series Devices*.

No special configuration beyond device initialization is required before configuring this feature.

### Overview

Data path debugging enhances troubleshooting capabilities by providing tracing and debugging at multiple processing units along the packet-processing path. With the data

path debugging feature, you can trace and debug (capture packets) at different data points along the processing path. At each event, you can specify an action (count, packet dump, packet summary, and trace) and you can set filters to define what packets to capture.

In this example, you define a traffic filter, then you apply an action profile. The action profile specifies a variety of actions on the processing unit. The NP ingress and NP egress are specified as location on the processing path to capture the data for incoming and outgoing traffic.

Next, you enable data path debugging in operational mode, and finally you view the data capture report.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security datapath-debug traceoptions file e2e.trace size 10m
set security datapath-debug capture-file datapcap format pcap
set security datapath-debug maximum-capture-size 1500
set security datapath-debug action-profile profile-1 preserve-trace-order
set security datapath-debug action-profile profile-1 record-pic-history
set security datapath-debug action-profile profile-1 event np-ingress trace
set security datapath-debug action-profile profile-1 event np-ingress count
set security datapath-debug action-profile profile-1 event np-ingress packet-summary
set security datapath-debug action-profile profile-1 event np-ingress packet-count
set security datapath-debug action-profile profile-1 event np-egress trace
set security datapath-debug action-profile profile-1 event np-egress count
set security datapath-debug action-profile profile-1 event np-egress packet-summary
set security datapath-debug action-profile profile-1 event np-egress packet-count
set security datapath-debug packet-filter filter-1
set security datapath-debug packet-filter filter-1 action-profile profile-1
set security datapath-debug packet-filter filter-1 protocol tcp
set security datapath-debug packet-filter filter-1 source-prefix 200.7.6.0/24
set security datapath-debug packet-filter filter-1 destination-prefix 200.8.6.0/24
set security datapath-debug packet-filter filter-1 source-port 1000
set security datapath-debug packet-filter filter-1 destination-port 80
set security datapath-debug packet-filter filter-1 interface xe-2/2/0.0
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure data path debugging:

1. Edit the security datapath-debug option for the multiple processing units along the packet-processing path:  

```
[edit]
user@host# edit security datapath-debug
```
2. Enable the capture file, file format, file size, and the number of files.



```
[edit security datapath-debug]
user@host# set traceoptions file e2e.trace size 10m
user@host# set capture-file datapcap format pcap;
user@host# set maximum-capture-size 1500
```

3. Configure action profile, event type, and actions for the action profile.

```
[edit security datapath-debug]
user@host# set action-profile profile-1 preserve-trace-order
user@host# set action-profile profile-1 record-pic-history
user@host# set action-profile profile-1 event np-ingress trace
user@host# set action-profile profile-1 event np-ingress count
user@host# set action-profile profile-1 event np-ingress packet-summary
user@host# set action-profile profile-1 event np-ingress packet-count
user@host# set action-profile profile-1 event np-egress trace
user@host# set action-profile profile-1 event np-egress count
user@host# set action-profile profile-1 event np-egress packet-summary
user@host# set action-profile profile-1 event np-egress packet-count
```

4. Configure packet filter, action, and filter options.

```
[edit security datapath-debug]
user@host# set packet-filter filter-1
user@host# set packet-filter filter-1 action-profile profile-1
user@host# set packet-filter filter-1 protocol tcp
user@host# set packet-filter filter-1 source-prefix 200.7.6.0/24
user@host# set packet-filter filter-1 destination-prefix 200.8.6.0/24
user@host# set packet-filter filter-1 source-port 1000
user@host# set packet-filter filter-1 destination-port 80
user@host# set packet-filter filter-1 interface xe-2/2/0.0
```

**Results** From configuration mode, confirm your configuration by entering the **show security datapath-debug** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
traceoptions {
 file e2e.trace size 10m;
}
capture-file datapcap format pcap;
maximum-capture-size 1500;
action-profile {
 profile-1 {
 preserve-trace-order;
 record-pic-history;
 event np-ingress {
 trace;
 count;
 packet-summary;
 packet-dump;
 }
 event np-egress {
 trace;
 count;
 packet-summary;
 packet-dump;
 }
 }
}
```

```
}
}
packet-filter filter-1 {
 action-profile profile-1;
 protocol tcp;
 source-prefix 200.7.6.0/24;
 destination-prefix 200.8.6.0/24;
 source-port 1000;
 destination-port 80;
 interface xe-2/2/0.0;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Enabling Data Path Debugging

- Step-by-Step Procedure** After configuring data path debugging, you must start the process on the device from operational mode.
1. Enable data path debugging.  

```
user@host> request security datapath-debug capture start
```

datapath-debug capture started on file datapcap
  2. Once you are done, you must disable data path debugging before you verify the configuration and view the reports.  

```
user@host> request security datapath-debug capture stop
```

datapath-debug capture successfully stopped, use show security datapath-debug capture to view

## Verification

Confirm that the configuration is working properly.

### Verifying Data Path Debug Packet Capture Details

---

**Purpose** Verify the data captured by enabling the data path debugging configuration.

**Action** From operational mode, enter the **show security datapath-debug capture** command.

```
Packet 8, len 152: (C2/F2/P0/SEQ:57935:np-ingress)
00 10 db ff 10 02 00 30 48 83 8d 4f 08 00 45 00
00 54 00 00 40 00 40 01 9f c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37
Packet 9, len 152: (C2/F2/P0/SEQ:57935:np-egress)
00 30 48 8d 1a bf 00 10 db ff 10 03 08 00 45 00
00 54 00 00 40 00 3f 01 a0 c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
```

```
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37....
```

For brevity, the **show** command output is truncated to display only a few samples. Additional samples have been replaced with ellipses (...).

To view the results, from CLI operational mode, access the local UNIX shell and navigate to the directory `/var/log/<file-name>`. The result can be read by using the **tcpdump** utility.

**Related Documentation**

- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)

## Understanding Security Debugging Using Trace Options

The Junos OS trace function allows applications to write security debugging information to a file. The information that appears in this file is based on criteria you set. You can use this information to analyze security application issues.

The trace function operates in a distributed manner, with each thread writing to its own trace buffer. These trace buffers are then collected at one point, sorted, and written to trace files. Trace messages are delivered using the InterProcess Communications (IPC) protocol. A trace message has a lower priority than that of control protocol packets such as BGP, OSPF, and IKE, and therefore delivery is not considered to be as reliable.

**Related Documentation**

- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)
- [Understanding Flow Debugging Using Trace Options on page 1905](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1899](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1894](#)
- [Displaying Output for Security Trace Options on page 1901](#)

## Setting Security Trace Options (CLI Procedure)

Use the following configuration statements to configure security trace options in the CLI configuration editor.

- To disable remote tracing, enter the following statement:

```
[edit]
user@host# set security traceoptions no-remote-trace
```

- To write trace messages to a local file, enter the following statement. The system saves the trace file in the `/var/log/` directory.

```
[edit]
user@host# set security traceoptions use-local-files
```

- To specify a name for the trace file, enter the following statement. Valid values range from 1 and 1024 characters. The name cannot include spaces, /, or % characters. The default filename is security.

```
[edit]
```

**user@host# set security traceoptions file *filename***

- To specify the maximum number of trace files that can accumulate, enter the following statement. Valid values range from 2 to 1000. The default value is 3.

**[edit]**

**user@host# set security traceoptions file files 3**

- To specify the match criteria that you want the system to use when logging information to the file, enter the following statement. Enter a regular expression. Wildcard (\*) characters are accepted.

**[edit]**

**user@host# set security traceoptions file match \*thread**

- To allow any user to read the trace file, enter the **world-readable** statement. Otherwise, enter the **no-world-readable** statement.

**[edit]**

**user@host# set security traceoptions file world-readable**

**user@host# set security traceoptions file no-world-readable**

- To specify the maximum size to which the trace file can grow, enter the following statement. Once the file reaches the specified size, it is compressed and renamed *filename0.gz*, the next file is named *filename1.gz*, and so on. Valid values range from 10240 to 1,073,741,824.

**[edit]**

**user@host# set security traceoptions file size 10240**

- To turn on trace options and to perform more than one tracing operation, set the following flags.

**[edit]**

**user@host# set security traceoptions flag all**

**user@host# set security traceoptions flag compilation**

**user@host# set security traceoptions flag configuration**

**user@host# set security traceoptions flag routing-socket**

- To specify the groups that these trace option settings do or do not apply to, enter the following statements:

**[edit]**

**user@host# set security traceoptions apply-groups *value***

**user@host# set security traceoptions apply-groups-except *value***

#### Related Documentation

- [Understanding Security Debugging Using Trace Options on page 1899](#)
- [Displaying Output for Security Trace Options on page 1901](#)

---

## Displaying Log and Trace Files

Enter the **monitor start** command to display real-time additions to system logs and trace files:

**user@host> monitor start *filename***

When the device adds a record to the file specified by *filename*, the record displays on the screen. For example, if you have configured a system log file named **system-log** (by including the **syslog** statement at the [edit system] hierarchy level), you can enter the **monitor start system-log** command to display the records added to the system log.

To display a list of files that are being monitored, enter the **monitor list** command. To stop the display of records for a specified file, enter the **monitor stop filename** command.

- Related Documentation**
- [Displaying a List of Devices on page 1906](#)
  - [Displaying Real-Time Monitoring Information on page 1757](#)

## Displaying Output for Security Trace Options

**Purpose** Display output for security trace options.

**Action** Use the **show security traceoptions** command to display the output of your trace files. For example:

```
[edit]
user@host # show security traceoptions file usp_trace
user@host # show security traceoptions flag all
user@host # show security traceoptions rate-limit 888
```

The output for this example is as follows:

```
Apr 11 16:06:42 21:13:15.750395:CID-906489336:FPC-01:PIC-01:THREAD_ID-01:PFE:now
update 0x3607edf8df8in 0x3607e8d0
Apr 11 16:06:42 21:13:15.874058:CID-1529687608:FPC-01:PIC-01:THREAD_ID-01:CTRL:Enter
Function[util_ssam_handler]
Apr 11 16:06:42 21:13:15.874485:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1: Rate
limit changed to 888
Apr 11 16:06:42 21:13:15.874538:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1:
Destination ID set to 1
Apr 11 16:06:42 21:13:15.874651:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2: Rate
limit changed to 888
Apr 11 16:06:42 21:13:15.874832:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2:
Destination ID set to 1
Apr 11 16:06:42 21:13:15.874942:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3: Rate
limit changed to 888
Apr 11 16:06:42 21:13:15.874997:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3:
Destination ID set to 1
```

- Related Documentation**
- [Understanding Security Debugging Using Trace Options on page 1899](#)
  - [Setting Security Trace Options \(CLI Procedure\) on page 1899](#)

## Displaying Multicast Trace Operations

To monitor and display multicast trace operations, enter the **mtrace monitor** command:

```
user@host> mtrace monitor
```

```
Mtrace query at Apr 21 16:00:54 by 192.1.30.2, resp to 224.0.1.32, qid 2a83aa
packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to 192.1.4.1 via group
224.1.1.1 (mxhop=60) Mtrace query at Apr 21 16:00:57 by 192.1.30.2, resp to
224.0.1.32, qid 25dc17 packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to
192.1.4.1 via group 224.1.1.1 (mxhop=60) Mtrace query at Apr 21 16:01:00 by
192.1.30.2, resp to same, qid 20e046 packet from 192.1.30.2 to 224.0.0.2 from
192.1.30.2 to 192.1.4.1 via group 224.1.1.1 (mxhop=60) Mtrace query at Apr 21
16:01:10 by 192.1.30.2, resp to same, qid 1d25ad packet from 192.1.30.2 to
224.0.0.2 from 192.1.30.2 to 192.1.4.1 via group 224.1.1.1 (mxhop=60)
```

This example displays only **mtrace** queries. However, when the device captures an **mtrace** response, the display is similar, but the complete **mtrace** response also appears (exactly as it is appears in the **mtrace from-source** command output).

Table 212 summarizes the output fields of the display.

Table 212: CLI mtrace monitor Command Output Summary

| Field                                       | Description                                                                                                                                                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mtrace operation-type at time-of-day</b> | <ul style="list-style-type: none"> <li><b>operation-type</b>—Type of multicast trace operation: <b>query</b> or <b>response</b>.</li> <li><b>time-of-day</b>—Date and time the multicast trace query or response was captured.</li> </ul> |
| <b>by</b>                                   | IP address of the host issuing the query.                                                                                                                                                                                                 |
| <b>resp to address</b>                      | <b>address</b> —Response destination address.                                                                                                                                                                                             |
| <b>qid qid</b>                              | <b>qid</b> —Query ID number.                                                                                                                                                                                                              |
| <b>packet from source to destination</b>    | <ul style="list-style-type: none"> <li><b>source</b>—IP address of the source of the query or response.</li> <li><b>destination</b>—IP address of the destination of the query or response.</li> </ul>                                    |
| <b>from source to destination</b>           | <ul style="list-style-type: none"> <li><b>source</b>—IP address of the multicast source.</li> <li><b>destination</b>—IP address of the multicast destination.</li> </ul>                                                                  |
| <b>via group address</b>                    | <b>address</b> —Group address being traced.                                                                                                                                                                                               |
| <b>mxhop=number</b>                         | <b>number</b> —Maximum hop setting.                                                                                                                                                                                                       |

- Related Documentation**
- [Using the J-Web Traceroute Tool on page 1902](#)
  - [J-Web Traceroute Results and Output Summary on page 1904](#)

## Using the J-Web Traceroute Tool

You can use the traceroute diagnostic tool to display a list of devices between the device and a specified destination host. The output is useful for diagnosing a point of failure in the path from the device to the destination host, and addressing network traffic latency and throughput problems.

The device generates the list of devices by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive device is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each device along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

To use the traceroute tool:

1. Select **Troubleshoot>Traceroute**.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Traceroute page (see [Table 213](#)).

**Table 213: Traceroute Field Summary**

| Field                   | Function                                                                                                                                                                                                                                                                                     | Your Action                                                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Host             | Identifies the destination host of the traceroute.<br><br>The <b>Remote Host</b> field is the only required field.                                                                                                                                                                           | Type the hostname or IP address of the destination host.                                                                                                                                                                                                                           |
| <b>Advanced Options</b> |                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                    |
| Don't Resolve Addresses | Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses.                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• Suppress the display of the hop hostnames by selecting the check box.</li> <li>• Display the hop hostnames by clearing the check box.</li> </ul>                                                                                          |
| Gateway                 | Specifies the IP address of the gateway to route through.                                                                                                                                                                                                                                    | Type the gateway IP address.                                                                                                                                                                                                                                                       |
| Source Address          | Specifies the source address of the outgoing traceroute packets.                                                                                                                                                                                                                             | Type the source IP address.                                                                                                                                                                                                                                                        |
| Bypass Routing          | Determines whether traceroute packets are routed by means of the routing table.<br><br>If the routing table is not used, traceroute packets are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, traceroute responses are not sent. | <ul style="list-style-type: none"> <li>• Bypass the routing table and send the traceroute packets to hosts on the specified interface only by selecting the check box.</li> <li>• Route the traceroute packets by means of the routing table by clearing the check box.</li> </ul> |
| Interface               | Specifies the interface on which the traceroute packets are sent.                                                                                                                                                                                                                            | Select the interface on which traceroute packets are sent from the list. If you select <b>any</b> , the traceroute requests are sent on all interfaces.                                                                                                                            |
| Time-to-Live            | Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.                                                                                                                                                                                                        | Select the TTL from the list.                                                                                                                                                                                                                                                      |
| Type-of-Service         | Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.                                                                                                                                                                                      | Select the decimal value of the TOS field from the list.                                                                                                                                                                                                                           |
| Resolve AS Numbers      | Determines whether the autonomous system (AS) number of each intermediate hop between the device and the destination host is displayed.                                                                                                                                                      | <ul style="list-style-type: none"> <li>• Display the AS numbers by selecting the check box.</li> <li>• Suppress the display of the AS numbers by clearing the check box.</li> </ul>                                                                                                |

4. Click **Start**.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

*hop-number host (ip-address) [as-number]time1 time2 time3*

The device sends a total of three traceroute packets to each router along the path and the round-trip time for each traceroute operation appears. If the device times out before receiving a **Time Exceeded** message, an asterisk (\*) appears for that round-trip time.

5. You can stop the traceroute operation before it is complete by clicking **OK** while the results of the traceroute operation appear.

#### Related Documentation

- [Diagnostic Tools Overview on page 1398](#)
- [J-Web Traceroute Results and Output Summary on page 1904](#)
- [Using the J-Web Ping MPLS Tool on page 1917](#)
- [Using the J-Web Ping Host Tool on page 1914](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)
- [Interfaces Feature Guide for Security Devices](#)

## J-Web Traceroute Results and Output Summary

Table 214 summarizes the output in the traceroute display.

Table 214: J-Web Traceroute Results and Output Summary

| Field             | Description                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>hop-number</i> | Number of the hop (device) along the path.                                                                                                                   |
| <i>host</i>       | Hostname, if available, or IP address of the device. If the Don't Resolve Addresses check box is selected, the hostname does not appear.                     |
| <i>ip-address</i> | IP address of the device.                                                                                                                                    |
| <i>as-number</i>  | AS number of the device.                                                                                                                                     |
| <i>time1</i>      | Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.  |
| <i>time2</i>      | Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device. |
| <i>time3</i>      | Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.  |



If the device does not display the complete path to the destination host, one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host, or a router along the path, might be configured to ignore ICMP traceroute messages.
- The host, or a device along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses.
- The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message.

**Related  
Documentation**

- [Diagnostic Tools Overview on page 1398](#)
- [Using the J-Web Traceroute Tool on page 1902](#)
- *Interfaces Feature Guide for Security Devices*

---

## Understanding Flow Debugging Using Trace Options

For flow trace options, you can define a packet filter using combinations of **destination-port**, **destination-prefix**, **interface**, **protocol**, **source-port**, and **source-prefix**. If the security flow trace flag for a certain module is set, the packet matching the specific packet filter triggers flow tracing and writes debugging information to the trace file.

**Related  
Documentation**

- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)
- [Understanding Security Debugging Using Trace Options on page 1899](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1905](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1894](#)

---

## Setting Flow Debugging Trace Options (CLI Procedure)

The following examples display the options you can set by using **security flow traceoptions**.

- To match the imap destination port for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-port imap
```

- To set the 1.2.3.4 destination IPv4 prefix address for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-prefix 1.2.3.4
```

- To set the fxp0 logical interface for the filter1 packet filter, use the following statement:

```
[edit]
```

```
user@host# set security flow traceoptions packet-filter filter1 interface fxp0
```

- To match the TCP IP protocol for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 protocol tcp
```

- To match the HTTP source port for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-port http
```

- To set the 5.6.7.8 IPv4 prefix address for the filter1 packet filter, use the following statement:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-prefix 5.6.7.8
```

#### Related Documentation

- [Understanding Flow Debugging Using Trace Options on page 1905](#)

## Displaying a List of Devices

To display a list of devices between the device and a specified destination host, enter the **traceroute** command with the following syntax:

```
user@host> traceroute host <interface interface-name> <as-number-lookup>
<bypass-routing> <gateway address> <inet | inet6> <no-resolve>
<routing-instance routing-instance-name> <source source-address> <tos number>
<tll number> <wait seconds>
```

[Table 215](#) describes the **traceroute** command options.

**Table 215: CLI traceroute Command Options**

| Option                          | Description                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host</i>                     | Sends traceroute packets to the hostname or IP address you specify.                                                                                                                                                                                                                                                      |
| <i>interface interface-name</i> | (Optional) Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.                                                                                                                                                                  |
| <i>as-number-lookup</i>         | (Optional) Displays the autonomous system (AS) number of each intermediate hop between the device and the destination host.                                                                                                                                                                                              |
| <i>bypass-routing</i>           | (Optional) Bypasses the routing tables and sends the traceroute packets only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.<br><br>Use this option to display a route to a local system through an interface that has no route through it. |
| <i>gateway address</i>          | (Optional) Uses the gateway you specify to route through.                                                                                                                                                                                                                                                                |
| <i>inet</i>                     | (Optional) Forces the traceroute packets to an IPv4 destination.                                                                                                                                                                                                                                                         |
| <i>inet6</i>                    | (Optional) Forces the traceroute packets to an IPv6 destination.                                                                                                                                                                                                                                                         |

Table 215: CLI traceroute Command Options (*continued*)

| Option                                                  | Description                                                                                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>no-resolve</b>                                       | (Optional) Suppresses the display of the hostnames of the hops along the path.                                                 |
| <b>routing-instance</b><br><i>routing-instance-name</i> | (Optional) Uses the routing instance you specify for the traceroute.                                                           |
| <b>source address</b>                                   | (Optional) Uses the source address that you specify, in the traceroute packet.                                                 |
| <b>tos number</b>                                       | (Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255. |
| <b>ttl number</b>                                       | (Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 128.                |
| <b>wait seconds</b>                                     | (Optional) Sets the maximum time to wait for a response.                                                                       |

To quit the **traceroute** command, press Ctrl-C.

The following is sample output from a **traceroute** command:

```

user@host> traceroute host2

traceroute to 173.24.232.66 (172.24.230.41), 30 hops max, 40 byte packets 1
173.18.42.253 (173.18.42.253) 0.482 ms 0.346 ms 0.318 ms 2 host4.site1.net
(173.18.253.5) 0.401 ms 0.435 ms 0.359 ms 3 host5.site1.net (173.18.253.5)
0.401 ms 0.360 ms 0.357 ms 4 173.24.232.65 (173.24.232.65) 0.420 ms 0.456
ms 0.378 ms 5 173.24.232.66 (173.24.232.66) 0.830 ms 0.779 ms 0.834 ms

```

The fields in the display are the same as those displayed by the J-Web traceroute diagnostic tool.

**Related Documentation**

- [Displaying Log and Trace Files on page 1900](#)



# Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits

- [MPLS Connection Checking Overview on page 1909](#)
- [Configuring Ping MPLS on page 1911](#)
- [Using the ping Command on page 1912](#)
- [Using the J-Web Ping Host Tool on page 1914](#)
- [J-Web Ping Host Results and Output Summary on page 1916](#)
- [Using the J-Web Ping MPLS Tool on page 1917](#)
- [J-Web Ping MPLS Results and Output Summary on page 1920](#)
- [Pinging Layer 2 Circuits on page 1921](#)
- [Pinging Layer 2 VPNs on page 1922](#)
- [Pinging Layer 3 VPNs on page 1923](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1924](#)

## MPLS Connection Checking Overview

---

Use either the J-Web ping MPLS diagnostic tool or the CLI commands **ping mpls**, **ping mpls l2circuit**, **ping mpls l2vpn**, and **ping mpls l3vpn** to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits.

Based on how the LSP or VPN outbound (egress) node at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP or VPN.

Each probe is an echo request sent to the LSP or VPN exit point as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the device receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

[Table 216](#) summarizes the options for using either the J-Web ping MPLS diagnostic tool or the CLI **ping mpls** command to display information about MPLS connections in VPNs and LSPs.

Table 216: Options for Checking MPLS Connections

| J-Web Ping MPLS Tool                        | ping mpls Command                   | Purpose                                                                                                                                                                                                                                                                                                                                 | Additional Information                                                                                                                                                                            |
|---------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ping RSVP-signaled LSP                      | ping mpls rsvp                      | Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The device pings a particular LSP using the configured LSP name.                                                                                                                                                                     | When an RSVP-signaled LSP has several paths, the device sends the ping requests on the path that is currently active.                                                                             |
| Ping LDP-signaled LSP                       | ping mpls ldp                       | Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The device pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.                                                                                                                                       | When an LDP-signaled LSP has several gateways, the device sends the ping requests through the first gateway.<br><br>Ping requests sent to LDP-signaled LSPs use only the master routing instance. |
| Ping LSP to Layer 3 VPN prefix              | ping mpls l3vpn                     | Checks the operability of the connections related to a Layer 3 VPN. The device tests whether a prefix is present in a provider edge (PE) device's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix.                                                                                                 | The device does not test the connection between a PE device and a customer edge (CE) router.                                                                                                      |
| Locate LSP using interface name             | ping mpls l2vpn interface           | Checks the operability of the connections related to a Layer 2 VPN. The device directs outgoing request probes out the specified interface.                                                                                                                                                                                             | —                                                                                                                                                                                                 |
| Instance to which this connection belongs   | ping mpls l2vpn instance            | Checks the operability of the connections related to a Layer 2 VPN. The device pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, to test the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound and outbound PE routers. | —                                                                                                                                                                                                 |
| Locate LSP from interface name              | ping mpls l2circuit interface       | Checks the operability of the Layer 2 circuit connections. The device directs outgoing request probes out the specified interface.                                                                                                                                                                                                      | —                                                                                                                                                                                                 |
| Locate LSP from virtual circuit information | ping mpls l2circuit virtual-circuit | Checks the operability of the Layer 2 circuit connections. The device pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE router, testing the integrity of the Layer 2 circuit between the inbound and outbound PE routers.                                                                 | —                                                                                                                                                                                                 |

Table 216: Options for Checking MPLS Connections (*continued*)

| J-Web Ping MPLS Tool  | ping mpls Command       | Purpose                                                                                                                                     | Additional Information |
|-----------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Ping end point of LSP | ping mpls lsp-end-point | Checks the operability of an LSP endpoint. The device pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address. | —                      |

- Related Documentation**
- [Diagnostic Tools Overview on page 1398](#)
  - [Configuring Ping MPLS on page 1911](#)
  - [Using the J-Web Ping Host Tool on page 1914](#)
  - [Using the ping Command on page 1912](#)

## Configuring Ping MPLS

Before using the ping MPLS feature, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and that the loopback interface on the outbound node is configured as **127.0.0.1**. The source address for MPLS probes must be a valid address on the device.

- **MPLS Enabled**—To process ping MPLS requests, the remote endpoint of the VPN or LSP must be configured appropriately. You must enable MPLS on the receiving interface of the outbound node for the VPN or LSP. If MPLS is not enabled, the remote endpoint drops the incoming request packets and returns an “ICMP host unreachable” message to the device.
- **Loopback Address**—The loopback address (**lo0**) on the outbound node must be configured as **127.0.0.1**. If this interface address is not configured correctly, the outbound node does not have this forwarding entry. It drops the incoming request packets and returns a “host unreachable” message to the device.
- **Source Address for Probes**—The source IP address you specify for a set of probes must be an address configured on one of the device interfaces. If it is not a valid device address, the ping request fails with the error message “Can’t assign requested address.”

- Related Documentation**
- [Diagnostic Tools Overview on page 1398](#)
  - [MPLS Connection Checking Overview on page 1909](#)
  - [Using the J-Web Ping Host Tool on page 1914](#)
  - [Using the J-Web Ping MPLS Tool on page 1917](#)
  - [Using the ping Command on page 1912](#)

## Using the ping Command

You can perform certain tasks only through the CLI. Use the CLI **ping** command to verify that a host can be reached over the network. This command is useful for diagnosing host and network connectivity problems. The device sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Enter the **ping** command with the following syntax:

```
user@host> ping host <interface source-interface> <bypass-routing> <count number>
<do-not-fragment> <inet | inet6> <interval seconds> <loose-source [hosts]>
<no-resolve> <pattern string> <rapid> <record-route>
<routing-instance routing-instance-name> <size bytes> <source source-address> <strict>
<strict-source [hosts]> <tos number> <tll number> <wait seconds> <detail> <verbose>
```

Table 217 describes the **ping** command options.

To quit the **ping** command, press Ctrl-C.

**Table 217: CLI ping Command Options**

| Option                            | Description                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host</i>                       | Pings the hostname or IP address you specify.                                                                                                                                                                                                                                                         |
| <i>interface source-interface</i> | (Optional) Sends the ping requests on the interface you specify. If you do not include this option, ping requests are sent on all interfaces.                                                                                                                                                         |
| <i>bypass-routing</i>             | (Optional) Bypasses the routing tables and sends the ping requests only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.<br><br>Use this option to ping a local system through an interface that has no route through it. |
| <i>count number</i>               | (Optional) Limits the number of ping requests to send. Specify a count from 1 through 2,000,000,000. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.                                                                                                       |
| <i>do-not-fragment</i>            | (Optional) Sets the Don't Fragment (DF) bit in the IP header of the ping request packet.                                                                                                                                                                                                              |
| <i>inet</i>                       | (Optional) Forces the ping requests to an IPv4 destination.                                                                                                                                                                                                                                           |
| <i>inet6</i>                      | (Optional) Forces the ping requests to an IPv6 destination.                                                                                                                                                                                                                                           |
| <i>interval seconds</i>           | (Optional) Sets the interval between ping requests, in seconds. Specify an interval from 0.1 through 10,000. The default value is 1 second.                                                                                                                                                           |
| <i>loose-source [hosts]</i>       | (Optional) For IPv4, sets the loose source routing option in the IP header of the ping request packet.                                                                                                                                                                                                |
| <i>no-resolve</i>                 | (Optional) Suppresses the display of the hostnames of the hops along the path.                                                                                                                                                                                                                        |
| <i>pattern string</i>             | (Optional) Includes the hexadecimal string you specify, in the ping request packet.                                                                                                                                                                                                                   |



Table 217: CLI ping Command Options (*continued*)

| Option                                                  | Description                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rapid</b>                                            | (Optional) Sends ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the <b>count</b> option. |
| <b>record-route</b>                                     | (Optional) For IPv4, sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed on the screen.                                                                                       |
| <b>routing-instance</b><br><b>routing-instance-name</b> | (Optional) Uses the routing instance you specify for the ping request.                                                                                                                                                                                                              |
| <b>size bytes</b>                                       | (Optional) Sets the size of the ping request packet. Specify a size from <b>0</b> through <b>65,468</b> . The default value is <b>56</b> bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.                                          |
| <b>source source-address</b>                            | (Optional) Uses the source address that you specify, in the ping request packet.                                                                                                                                                                                                    |
| <b>strict</b>                                           | (Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.                                                                                                                                                                             |
| <b>strict-source [hosts]</b>                            | (Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet, and uses the list of hosts you specify for routing the packet.                                                                                                              |
| <b>tos number</b>                                       | (Optional) Sets the type-of-service (TOS) value in the IP header of the ping request packet. Specify a value from <b>0</b> through <b>255</b> .                                                                                                                                     |
| <b>ttl number</b>                                       | (Optional) Sets the time-to-live (TTL) value for the ping request packet. Specify a value from <b>0</b> through <b>255</b> .                                                                                                                                                        |
| <b>wait seconds</b>                                     | (Optional) Sets the maximum time to wait after sending the last ping request packet. If you do not specify this option, the default delay is <b>10</b> seconds. If you use this option without the <b>count</b> option, the device uses a default count of <b>5</b> packets.        |
| <b>detail</b>                                           | (Optional) Displays the interface on which the ping response was received.                                                                                                                                                                                                          |
| <b>verbose</b>                                          | (Optional) Displays detailed output.                                                                                                                                                                                                                                                |

The following is sample output from a **ping** command:

```

user@host> ping host3 count 4

PING host3.site.net (176.26.232.111): 56 data bytes 64 bytes from 176.26.232.111:
icmp_seq=0 ttl=122 time=0.661 ms 64 bytes from 176.26.232.111: icmp_seq=1 ttl=122
time=0.619 ms 64 bytes from 176.26.232.111: icmp_seq=2 ttl=122 time=0.621 ms 64
bytes from 176.26.232.111: icmp_seq=3 ttl=122 time=0.634 ms --- host3.site.net
ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms

```

The fields in the display are the same as those displayed by the J-Web ping host diagnostic tool.

- Related Documentation**
- [Diagnostic Tools Overview on page 1398](#)
  - [Configuring Ping MPLS on page 1911](#)
  - [Pinging Layer 2 Circuits on page 1921](#)
  - [Pinging Layer 2 VPNs on page 1922](#)
  - [Pinging Layer 3 VPNs on page 1923](#)
  - [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1924](#)
  - *Interfaces Feature Guide for Security Devices*

## Using the J-Web Ping Host Tool

You can ping a host to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The device sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

Alternatively, you can use the CLI **ping** command. (See [“Using the ping Command” on page 1912.](#))

To use the ping host tool:

1. Select **Troubleshoot>Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page (see [Table 218](#)).

**Table 218: J-Web Ping Host Field Summary**

| Field                   | Function                                                                           | Your Action                                                                                                                                                                               |
|-------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Host             | Identifies the host to ping.<br><br>This is the only required field.               | Type the hostname or IP address of the host to ping.                                                                                                                                      |
| <b>Advanced Options</b> |                                                                                    |                                                                                                                                                                                           |
| Don't Resolve Addresses | Determines whether to display hostnames of the hops along the path.                | <ul style="list-style-type: none"> <li>• Suppress the display of the hop hostnames by selecting the check box.</li> <li>• Display the hop hostnames by clearing the check box.</li> </ul> |
| Interface               | Specifies the interface on which the ping requests are sent.                       | Select the interface on which ping requests are sent from the list. If you select <b>any</b> , the ping requests are sent on all interfaces.                                              |
| Count                   | Specifies the number of ping requests to send.                                     | Select the number of ping requests to send from the list.                                                                                                                                 |
| Don't Fragment          | Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet. | <ul style="list-style-type: none"> <li>• Set the DF bit by selecting the check box.</li> <li>• Clear the DF bit by clearing the check box.</li> </ul>                                     |

Table 218: J-Web Ping Host Field Summary (*continued*)

| Field            | Function                                                                                                                                                                                                                                                                            | Your Action                                                                                                                                                                                                                                                    |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Record Route     | Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.                                                                                                         | <ul style="list-style-type: none"> <li>Record and display the path of the packet by selecting the check box.</li> <li>Suppress the recording and display of the path of the packet by clearing the check box.</li> </ul>                                       |
| Type-of-Service  | Specifies the type-of-service (TOS) value in the IP header of the ping request packet.                                                                                                                                                                                              | Select the decimal value of the TOS field from the list.                                                                                                                                                                                                       |
| Routing Instance | Names the routing instance for the ping attempt.                                                                                                                                                                                                                                    | Select the routing instance name from the list.                                                                                                                                                                                                                |
| Interval         | Specifies the interval, in seconds, between the transmission of each ping request.                                                                                                                                                                                                  | Select the interval from the list.                                                                                                                                                                                                                             |
| Packet Size      | Specifies the size of the ping request packet.                                                                                                                                                                                                                                      | Type the size, in bytes, of the packet. The size can be from 0 through 65,468. The device adds 8 bytes of ICMP header to the size.                                                                                                                             |
| Source Address   | Specifies the source address of the ping request packet.                                                                                                                                                                                                                            | Type the source IP address.                                                                                                                                                                                                                                    |
| Time-to-Live     | Specifies the time-to-live (TTL) hop count for the ping request packet.                                                                                                                                                                                                             | Select the TTL from the list.                                                                                                                                                                                                                                  |
| Bypass Routing   | <p>Determines whether ping requests are routed by means of the routing table.</p> <p>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.</p> | <ul style="list-style-type: none"> <li>Bypass the routing table and send the ping requests to hosts on the specified interface only by selecting the check box.</li> <li>Route the ping requests using the routing table by clearing the check box.</li> </ul> |

4. Click **Start**.

The results of the ping operation appear in the main pane. If no options are specified, each ping response is in the following format:

*bytes bytes from ip-address: icmp\_seq=number ttl=number time=time*

5. You can stop the ping operation before it is complete by clicking **OK**.
**Related  
Documentation**

- [Diagnostic Tools Overview on page 1398](#)
- [Configuring Ping MPLS on page 1911](#)
- [J-Web Ping Host Results and Output Summary on page 1916](#)
- [Using the J-Web Traceroute Tool on page 1902](#)
- [Using the J-Web Ping MPLS Tool on page 1917](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)

## J-Web Ping Host Results and Output Summary

Table 219 summarizes the output in the ping host display.

Table 219: Ping Host Results and Output

| Ping Host Result                                                                       | Description                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>bytes bytes from ip-address</i>                                                     | <ul style="list-style-type: none"> <li><b>bytes</b>—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8.</li> <li><b>ip-address</b>—IP address of destination host that sent the ping response packet.</li> </ul>                                            |
| <i>icmp_seq=0</i><br><i>icmp_seq=number</i>                                            | <b>number</b> —Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.                                                                                                                                                        |
| <i>ttl=number</i>                                                                      | <b>number</b> —Time-to-live hop-count value of the ping response packet.                                                                                                                                                                                                                                      |
| <i>number packets transmitted</i>                                                      | <b>number</b> —Number of ping requests (probes) sent to host.                                                                                                                                                                                                                                                 |
| <i>percentage packet loss</i>                                                          | <b>percentage</b> —Number of ping responses divided by the number of ping requests, specified as a percentage.                                                                                                                                                                                                |
| <i>round-trip min/avg/max/stddev =</i><br><i>min-time/avg-time/max-time/std-dev ms</i> | <ul style="list-style-type: none"> <li><b>min-time</b>—Minimum round-trip time (see <b>time=time</b> field in this table).</li> <li><b>avg-time</b>—Average round-trip time.</li> <li><b>max-time</b>—Maximum round-trip time.</li> <li><b>std-dev</b>—Standard deviation of the round-trip times.</li> </ul> |

If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host might be configured to ignore ICMP echo requests.
- The host might be configured with a firewall filter that blocks ICMP echo requests or ICMP echo responses.
- The size of the ICMP echo request packet exceeds the MTU of a host along the path.
- The value you selected in the Time-to-Live box was less than the number of hops in the path to the host, in which case the host might reply with an ICMP error message.

### Related Documentation

- [Diagnostic Tools Overview on page 1398](#)
- [Configuring Ping MPLS on page 1911](#)
- [Using the J-Web Ping Host Tool on page 1914](#)
- *Interfaces Feature Guide for Security Devices*

## Using the J-Web Ping MPLS Tool

Before using the ping MPLS feature, make sure that the receiving interface on the VPN or LSP remote endpoint has MPLS enabled, and that the loopback interface on the outbound node is configured as **127.0.0.1**. The source address for MPLS probes must be a valid address on the device.

To use the ping MPLS tool:

1. Select **Troubleshoot>Ping MPLS** from the task bar.
2. Next to the ping MPLS option you want to use, click the expand icon.
3. Enter information into the Ping MPLS page (see [Table 220](#)).

**Table 220: J-Web Ping MPLS Field Summary**

| Field                                 | Function                                                         | Your Action                                                                          |
|---------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>Ping RSVP-signaled LSP</b>         |                                                                  |                                                                                      |
| LSP Name                              | Identifies the LSP to ping.                                      | Type the name of the LSP to ping.                                                    |
| Source Address                        | Specifies the source address of the ping request packet.         | Type the source IP address—a valid address configured on a device interface.         |
| Count                                 | Specifies the number of ping requests to send.                   | Select the number of ping requests to send from the list. The default is 5 requests. |
| Detailed Output                       | Requests the display of extensive rather than brief ping output. | Select the check box to display detailed output.                                     |
| <b>Ping LDP-signaled LSP</b>          |                                                                  |                                                                                      |
| FEC Prefix                            | Identifies the LSP to ping.                                      | Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping.    |
| Source Address                        | Specifies the source address of the ping request packet.         | Type the source IP address—a valid address configured on a device interface.         |
| Count                                 | Specifies the number of ping requests to send.                   | Select the number of ping requests to send from the list. The default is 5 requests. |
| Detailed Output                       | Requests the display of extensive rather than brief ping output. | Select the check box to display detailed output.                                     |
| <b>Ping LSP to Layer 3 VPN prefix</b> |                                                                  |                                                                                      |
| Layer 3 VPN Name                      | Identifies the Layer 3 VPN to ping.                              | Type the name of the VPN to ping.                                                    |
| Count                                 | Specifies the number of ping requests to send.                   | Select the number of ping requests to send from the list. The default is 5 requests. |

Table 220: J-Web Ping MPLS Field Summary (*continued*)

| Field                                            | Function                                                                | Your Action                                                                                                                                         |
|--------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Detailed Output                                  | Requests the display of extensive rather than brief ping output.        | Select the check box to display detailed output.                                                                                                    |
| VPN Prefix                                       | Identifies the IP address prefix and length of the Layer 3 VPN to ping. | Type the IP address prefix and length of the VPN to ping.                                                                                           |
| Source Address                                   | Specifies the source address of the ping request packet.                | Type the source IP address—a valid address configured on a device interface.                                                                        |
| <b>Locate LSP using interface name</b>           |                                                                         |                                                                                                                                                     |
| Interface                                        | Specifies the interface on which the ping requests are sent.            | Select the device interface on which ping requests are sent from the list. If you select <b>any</b> , the ping requests are sent on all interfaces. |
| Source Address                                   | Specifies the source address of the ping request packet.                | Type the source IP address—a valid address configured on a device interface.                                                                        |
| Count                                            | Specifies the number of ping requests to send.                          | Select the number of ping requests to send from the list. The default is 5 requests.                                                                |
| Detailed Output                                  | Requests the display of extensive rather than brief ping output.        | Select the check box to display detailed output.                                                                                                    |
| <b>Instance to which this connection belongs</b> |                                                                         |                                                                                                                                                     |
| Layer 2VPN Name                                  | Identifies the Layer 2 VPN to ping.                                     | Type the name of the VPN to ping.                                                                                                                   |
| Remote Site Identifier                           | Specifies the remote site identifier of the Layer 2 VPN to ping.        | Type the remote site identifier for the VPN.                                                                                                        |
| Source Address                                   | Specifies the source address of the ping request packet.                | Type the source IP address—a valid address configured on a device interface.                                                                        |
| Local Site Identifier                            | Specifies the local site identifier of the Layer 2 VPN to ping.         | Type the local site identifier for the VPN.                                                                                                         |
| Count                                            | Specifies the number of ping requests to send.                          | Select the number of ping requests to send from the list. The default is 5 requests.                                                                |
| Detailed Output                                  | Requests the display of extensive rather than brief ping output.        | Select the check box to display detailed output.                                                                                                    |
| <b>Locate LSP from interface name</b>            |                                                                         |                                                                                                                                                     |
| Interface                                        | Specifies the interface on which the ping requests are sent.            | Select the device interface on which ping requests are sent from the list. If you select <b>any</b> , the ping requests are sent on all interfaces. |
| Source Address                                   | Specifies the source address of the ping request packet.                | Type the source IP address—a valid address configured on a device interface.                                                                        |

Table 220: J-Web Ping MPLS Field Summary (*continued*)

| Field                                              | Function                                                                       | Your Action                                                                                     |
|----------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Count                                              | Specifies the number of ping requests to send.                                 | Select the number of ping requests to send from the list. The default is 5 requests.            |
| Detailed Output                                    | Requests the display of extensive rather than brief ping output.               | Select the check box to display detailed output.                                                |
| <b>Locate LSP from virtual circuit information</b> |                                                                                |                                                                                                 |
| Remote Neighbor                                    | Identifies the remote neighbor (PE device) within the virtual circuit to ping. | Type the IP address of the remote neighbor within the virtual circuit.                          |
| Circuit Identifier                                 | Specifies the virtual circuit identifier for the Layer 2 circuit to ping.      | Type the virtual circuit identifier for the Layer 2 circuit.                                    |
| Source Address                                     | Specifies the source address of the ping request packet.                       | Type the source IP address—a valid address configured on a device interface.                    |
| Count                                              | Specifies the number of ping requests to send.                                 | Select the number of ping requests to send from the list.                                       |
| Detailed Output                                    | Requests the display of extensive rather than brief ping output.               | Select the check box to display detailed output.                                                |
| <b>Ping end point of LSP</b>                       |                                                                                |                                                                                                 |
| VPN Prefix                                         | Identifies the LSP endpoint to ping.                                           | Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping. |
| Source Address                                     | Specifies the source address of the ping request packet.                       | Type the source IP address—a valid address configured on a device interface.                    |
| Count                                              | Specifies the number of ping requests to send.                                 | Select the number of ping requests to send from the list.                                       |
| Detailed Output                                    | Requests the display of extensive rather than brief ping output.               | Select the check box to display detailed output.                                                |

4. Click **Start**.
5. You can stop the ping operation before it is complete by clicking **OK**.

**Related Documentation**

- [Diagnostic Tools Overview on page 1398](#)
- [Configuring Ping MPLS on page 1911](#)
- [J-Web Ping MPLS Results and Output Summary on page 1920](#)
- [Using the J-Web Traceroute Tool on page 1902](#)
- [Using the J-Web Ping Host Tool on page 1914](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)

## J-Web Ping MPLS Results and Output Summary

Table 221 summarizes the output in the ping MPLS display.

**Table 221: J-Web Ping MPLS Results and Output Summary**

| Field                             | Description                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exclamation point (!)             | Echo reply was received.                                                                                                                                                                    |
| Period (.)                        | Echo reply was not received within the timeout period.                                                                                                                                      |
| x                                 | Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately.                                                 |
| <i>number packets transmitted</i> | <i>number</i> —Number of ping requests (probes) sent to a host.                                                                                                                             |
| <i>number packets received</i>    | <i>number</i> —Number of ping responses received from a host.                                                                                                                               |
| <i>percentage packet loss</i>     | <i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage.                                                                              |
| <i>time</i>                       | For Layer 2 circuits only, the number of milliseconds required for the ping packet to reach the destination. This value is approximate, because the packet has to reach the Routing Engine. |

If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host might be configured to ignore echo requests.
- The host might be configured with a firewall filter that blocks echo requests or echo responses.
- The size of the echo request packet exceeds the MTU of a host along the path.
- The outbound node at the remote endpoint is not configured to handle MPLS packets.
- The remote endpoint's loopback address is not configured to 127.0.0.1.

### Related Documentation

- [Diagnostic Tools Overview on page 1398](#)
- [Configuring Ping MPLS on page 1911](#)
- [Using the J-Web Ping MPLS Tool on page 1917](#)
- [Interfaces Feature Guide for Security Devices](#)



## Pinging Layer 2 Circuits

Enter the **ping mpls l2circuit** command with the following syntax:

```
user@host> ping mpls l2circuit (interface interface-name | virtual-circuit neighbor
 prefix-name virtual-circuit-id) <exp forwarding-class> <count number>
 <source source-address> <detail>
```

Table 222 describes the **ping mpls l2circuit** command options.

Table 222: CLI ping mpls l2circuit Command Options

| Option                                                                                              | Description                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l2circuit interface</b><br><i>interface-name</i>                                                 | Sends ping requests out the specified interface configured for the Layer 2 circuit on the outbound PE device.                                                                                                       |
| <b>l2circuit virtual-circuit</b><br><b>neighbor</b> <i>prefix-name</i><br><i>virtual-circuit-id</i> | Pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE device, testing the integrity of the Layer 2 circuit between the inbound and outbound PE devices.                   |
| <b>exp forwarding-class</b>                                                                         | (Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.                                                                                                                         |
| <b>count</b> <i>number</i>                                                                          | (Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C. |
| <b>source</b> <i>source-address</i>                                                                 | (Optional) Uses the source address that you specify, in the ping request packet.                                                                                                                                    |
| <b>detail</b>                                                                                       | (Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.                                |

To quit the **ping mpls l2circuit** command, press Ctrl-C.

The following is sample output from a **ping mpls l2circuit** command:

```
user@host> ping mpls l2circuit interface fe-1/0/0.0
```

```
Request for seq 1, to interface 69, labels <100000, 100208>
```

```
Reply for seq 1, return code: Egress-ok, time: 0.439 ms
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

### Related Documentation

- [Using the ping Command on page 1912](#)
- [Configuring Ping MPLS on page 1911](#)
- [Pinging Layer 2 VPNs on page 1922](#)
- [Pinging Layer 3 VPNs on page 1923](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1924](#)
- [Using the J-Web Ping Host Tool on page 1914](#)

## Pinging Layer 2 VPNs

Enter the **ping mpls l2vpn** command with the following syntax:

```
user@host> ping mpls l2vpn interface interface-name | instance l2vpn-instance-name
local-site-id local-site-id-number remote-site-id remote-site-id-number
<bottom-label-ttl> <exp forwarding-class> <count number> <source source-address>
<detail>
```

Table 223 describes the **ping mpls l2vpn** command options.

**Table 223: CLI ping mpls l2vpn Command Options**

| Option                                                                                                                                                              | Description                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l2vpn interface</b><br><i>interface-name</i>                                                                                                                     | Sends ping requests out the specified interface configured for the Layer 2 VPN on the outbound (egress) PE device.                                                                                                                                                 |
| <b>l2vpn instance</b><br><i>l2vpn-instance-name</i><br><i>local-site-id</i><br><i>local-site-id-number</i><br><i>remote-site-id</i><br><i>remote-site-id-number</i> | Pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, testing the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound (ingress) and outbound PE devices. |
| <b>bottom-label-ttl</b>                                                                                                                                             | (Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.                                                                                                                                                                     |
| <b>exp forwarding-class</b>                                                                                                                                         | (Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.                                                                                                                                                                        |
| <b>countnumber</b>                                                                                                                                                  | (Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.                                                |
| <b>source source-address</b>                                                                                                                                        | (Optional) Uses the source address that you specify, in the ping request packet.                                                                                                                                                                                   |
| <b>detail</b>                                                                                                                                                       | (Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.                                                                               |

To quit the **ping mpls l2vpn** command, press Ctrl-C.

The following is sample output from a **ping mpls l2vpn** command:

```
user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2 detail
Request for seq 1, to interface 68, labels <800001, 100176>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <800001, 100176>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <800001, 100176>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <800001, 100176>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <800001, 100176>
Reply for seq 5, return code: Egress-ok
```

```
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

#### Related Documentation

- [Using the ping Command on page 1912](#)
- [Configuring Ping MPLS on page 1911](#)
- [Pinging Layer 2 Circuits on page 1921](#)
- [Pinging Layer 3 VPNs on page 1923](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1924](#)
- [Using the J-Web Ping Host Tool on page 1914](#)

## Pinging Layer 3 VPNs

Enter the **ping mpls l3vpn** command with the following syntax:

```
user@host> ping mpls l3vpn prefix prefix-name <l3vpn-name> <bottom-label-ttl>
<exp forwarding-class> <count number> <source source-address> <detail>
```

[Table 224](#) describes the **ping mpls l3vpn** command options.

**Table 224: CLI ping mpls l3vpn Command Options**

| Option                                 | Description                                                                                                                                                                                                                   |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>l3vpn prefix <i>prefix-name</i></b> | Pings the remote host specified by the prefix to verify that the prefix is present in the PE device's VPN routing and forwarding (VRF) table. This option does not test the connectivity between a PE device and a CE device. |
| <b><i>l3vpn-name</i></b>               | (Optional) Layer 3 VPN name.                                                                                                                                                                                                  |
| <b>bottom-label-ttl</b>                | (Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.                                                                                                                                |
| <b>exp <i>forwarding-class</i></b>     | (Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.                                                                                                                                   |
| <b>count<i>number</i></b>              | (Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.           |
| <b>source <i>source-address</i></b>    | (Optional) Uses the source address that you specify, in the ping request packet.                                                                                                                                              |
| <b>detail</b>                          | (Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.                                          |

To quit the **ping mpls l3vpn** command, press Ctrl-C.

The following is sample output from a **ping mpls l3vpn** command:

```

user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

#### Related Documentation

- [Using the ping Command on page 1912](#)
- [Configuring Ping MPLS on page 1911](#)
- [Pinging Layer 2 Circuits on page 1921](#)
- [Pinging Layer 2 VPNs on page 1922](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1924](#)
- [Using the J-Web Ping Host Tool on page 1914](#)

## Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs

Enter the **ping mpls** command with the following syntax:

```

user@host> ping mpls (ldp fec | lsp-end-point prefix-name | rsvp lsp-name)
<exp forwarding-class> <count number> <source source-address> <detail>

```

[Table 225](#) describes the **ping mpls** command options.

**Table 225: CLI ping mpls ldp and ping mpls lsp-end-point Command Options**

| Option                           | Description                                                                                                                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ldp fec</b>                   | Pings an LDP-signaled LSP identified by the forwarding equivalence class (FEC) prefix and length.                                                                                                                   |
| <b>lsp-end-point prefix-name</b> | Pings an LSP endpoint using either an LDP FEC or a RSVP LSP endpoint address.                                                                                                                                       |
| <b>rsvp lsp-name</b>             | Pings an RSVP-signaled LSP identified by the specified LSP name.                                                                                                                                                    |
| <b>exp forwarding-class</b>      | (Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.                                                                                                                         |
| <b>countnumber</b>               | (Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C. |
| <b>source source-address</b>     | (Optional) Uses the source address that you specify, in the ping request packet.                                                                                                                                    |
| <b>detail</b>                    | (Optional) Displays detailed output about the echo requests sent and received. Detailed output includes the MPLS labels used for each request and the return codes for each request.                                |

To quit the **ping mpls** command, press Ctrl-C.

The following is sample output from a **ping mpls** command:

```
user@host> ping mpls rsvp count 5
```

```
!!xxx
```

```
--- lsping statistics ---
```

```
5 packets transmitted, 2 packets received, 60% packet loss
```

```
3 packets received with error status, not counted as received.
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool.

**Related  
Documentation**

- [Using the ping Command on page 1912](#)
- [Configuring Ping MPLS on page 1911](#)
- [Pinging Layer 2 Circuits on page 1921](#)
- [Pinging Layer 2 VPNs on page 1922](#)
- [Pinging Layer 3 VPNs on page 1923](#)
- [Using the J-Web Ping Host Tool on page 1914](#)



## CHAPTER 90

# Using Packet Capture to Analyze Network Traffic

- [Packet Capture Overview on page 1927](#)
- [Example: Enabling Packet Capture on a Device on page 1930](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Example: Configuring Packet Capture for Datapath Debugging on page 1937](#)
- [Disabling Packet Capture on page 1940](#)
- [Deleting Packet Capture Files on page 1941](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1941](#)
- [Displaying Packet Headers on page 1943](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)
- [J-Web Packet Capture Results and Output Summary on page 1950](#)

## Packet Capture Overview

---

Packet capture is a tool that helps you to analyze network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets traveling over the network for monitoring and logging.



**NOTE:** Packet capture is supported on physical interfaces, reth interfaces, and tunnel interfaces, such as gr, ip, st0, and lsq-/ls.

Packets are captured as binary data, without modification. You can read the packet information offline with a packet analyzer such as Ethereal or tcpdump. If you need to quickly capture packets destined for, or originating from, the Routing Engine and analyze them online, you can use the J-Web packet capture diagnostic tool.



**NOTE:** The packet capture tool does not support IPv6 packet capture.

You can use either the J-Web configuration editor or CLI configuration editor to configure packet capture.

Network administrators and security engineers use packet capture to perform the following tasks:

- Monitor network traffic and analyze traffic patterns.
- Identify and troubleshoot network problems.
- Detect security breaches in the network, such as unauthorized intrusions, spyware activity, or ping scans.

Packet capture operates like traffic sampling on the device, except that it captures entire packets including the Layer 2 header and saves the contents to a file in libpcap format. Packet capture also captures IP fragments. You cannot enable packet capture and traffic sampling on the device at the same time. Unlike traffic sampling, there are no tracing operations for packet capture.



**NOTE:** You can enable packet capture and port mirroring simultaneously on a device.

This section contains the following topics:

- [Packet Capture on Device Interfaces on page 1928](#)
- [Firewall Filters for Packet Capture on page 1929](#)
- [Packet Capture Files on page 1929](#)
- [Analysis of Packet Capture Files on page 1929](#)

## Packet Capture on Device Interfaces

Packet capture is supported on the T1, T3, E1, E3, serial, Fast Ethernet, ADSL, G.SHDSL, PPPoE, and ISDN interfaces.

To capture packets on an ISDN interface, configure packet capture on the dialer interface. To capture packets on a PPPoE interface, configure packet capture on the PPPoE logical interface.

Packet capture supports PPP, Cisco HDLC, Frame Relay, and other ATM encapsulations. Packet capture also supports Multilink PPP (MLPPP), Multilink Frame Relay end-to-end (MLFR), and Multilink Frame Relay UNI/NNI (MFR) encapsulations.

You can capture all IPv4 packets flowing on an interface in the inbound or outbound direction. However, on traffic that bypasses the flow software module (protocol packets such as ARP, OSPF, and PIM), packets generated by the Routing Engine are not captured unless you have configured and applied a firewall filter on the interface in the outbound direction.



Tunnel interfaces can support packet capture in the outbound direction only.

Use the J-Web configuration editor or CLI configuration editor to specify the maximum packet size, the filename to be used for storing the captured packets, the maximum file size, the maximum number of packet capture files, and the file permissions.



**NOTE:** For packets captured on T1, T3, E1, E3, serial, and ISDN interfaces in the outbound (egress) direction, the size of the packet captured might be 1 byte less than the maximum packet size configured because of the packet loss priority (PLP) bit.

To modify encapsulation on an interface that has packet capture configured, you must first disable packet capture.

## Firewall Filters for Packet Capture

When you enable packet capture on a device, all packets flowing in the direction specified in packet capture configuration (inbound, outbound, or both) are captured and stored. Configuring an interface to capture all packets might degrade the performance of the device. You can control the number of packets captured on an interface with firewall filters and specify various criteria to capture packets for specific traffic flows.

You must also configure and apply appropriate firewall filters on the interface if you need to capture packets generated by the host device, because interface sampling does not capture packets originating from the host device.

## Packet Capture Files

When packet capture is enabled on an interface, the entire packet including the Layer 2 header is captured and stored in a file. You can specify the maximum size of the packet to be captured, up to 1500 bytes. Packet capture creates one file for each physical interface. You can specify the target filename, the maximum size of the file, and the maximum number of files.

File creation and storage take place in the following way. Suppose you name the packet capture file **pcap-file**. Packet capture creates multiple files (one per physical interface), suffixing each file with the name of the physical interface; for example, **pcap-file.fe-0.0.1** for the Fast Ethernet interface **fe-0.0.1**. When the file named **pcap-file.fe-0.0.1** reaches the maximum size, the file is renamed **pcap-file.fe-0.0.1.0**. When the file named **pcap-file.fe-0.0.1** reaches the maximum size again, the file named **pcap-file.fe-0.0.1.0** is renamed **pcap-file.fe-0.0.1.1** and **pcap-file.fe-0.0.1** is renamed **pcap-file.fe-0.0.1.0**. This process continues until the maximum number of files is exceeded and the oldest file is overwritten. The **pcap-file.fe-0.0.1** file is always the latest file.

Packet capture files are not removed even after you disable packet capture on an interface.

## Analysis of Packet Capture Files

Packet capture files are stored in libpcap format in the **/var/tmp** directory. You can specify user or administrator privileges for the files.

Packet capture files can be opened and analyzed offline with tcpdump or any packet analyzer that recognizes the libpcap format. You can also use FTP or the Session Control Protocol (SCP) to transfer the packet capture files to an external device.



**NOTE:** Disable packet capture before opening the file for analysis or transferring the file to an external device with FTP or SCP. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

#### Related Documentation

- [Example: Enabling Packet Capture on a Device on page 1930](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)

---

## Example: Enabling Packet Capture on a Device

---

This example shows how to enable packet capture on a device, allowing you to analyze network traffic and troubleshoot network problems

- [Requirements on page 1930](#)
- [Overview on page 1930](#)
- [Configuration on page 1930](#)
- [Verification on page 1932](#)

### Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.

### Overview

In this example, you set the maximum packet capture size in each file as 500 bytes. The range is from 68 through 1500, and the default is 68 bytes. You specify the target filename for the packet capture file as pcap-file. You then specify the maximum number of files to capture as 100. The range is from 2 through 10,000, and the default is 10 files. You set the maximum size of each file to 1024 bytes. The range is from 1,024 through 104,857,600, and the default is 512,000 bytes. Finally, you specify that all users have permission to read the packet capture files.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set forwarding-options packet-capture maximum-capture-size 500
set forwarding-options packet-capture file filename pcap-file files 100 size 1024
world-readable
```

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To enable packet capture on a device:

1. Set the maximum packet capture size.  

```
[edit]
user@host# edit forwarding-options
user@host# set packet-capture maximum-capture-size 500
```
2. Specify the target filename.  

```
[edit forwarding-options]
user@host# set packet-capture file filename pcap-file
```
3. Specify the maximum number of files to capture.  

```
[edit forwarding-options]
user@host# set packet-capture file files 100
```
4. Specify the maximum size of each file.  

```
[edit forwarding-options]
user@host# set packet-capture file size 1024
```
5. Specify that all users have permission to read the file.  

```
[edit forwarding-options]
user@host# set packet-capture file world-readable
```

**Results** From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show forwarding-options
packet-capture {
 file filename pcap-file files 100 size 1k world-readable;
 maximum-capture-size 500;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Verifying the Packet Capture Configuration on page 1932](#)
- [Verifying Captured Packets on page 1932](#)

### Verifying the Packet Capture Configuration

**Purpose** Verify that the packet capture is configured on the device.

**Action** From configuration mode, enter the **show forwarding-options** command. Verify that the output shows the intended file configuration for capturing packets.

### Verifying Captured Packets

**Purpose** Verify that the packet capture file is stored under the **/var/tmp** directory and the packets can be analyzed offline.

**Action** 1. Disable packet capture.

Using FTP, transfer a packet capture file (for example, **126b.fe-0.0.1**), to a server where you have installed packet analyzer tools (for example, **tools-server**).

a. From configuration mode, connect to **tools-server** using FTP.

```
[edit]
user@host# run ftp tools-server
Connected to tools-server.mydomain.net
220 tools-server.mydomain.net FTP server (Version 6.00LS) ready
Name (tools-server:user):remoteuser
331 Password required for remoteuser.
Password:
230 User remoteuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

b. Navigate to the directory where packet capture files are stored on the device.

```
ftp> lcd /var/tmp
Local directory now /cf/var/tmp
```

c. Copy the packet capture file that you want to analyze to the server, for example **126b.fe-0.0.1**.

```
ftp> put 126b.fe-0.0.1
local: 126b.fe-0.0.1 remote: 126b.fe-0.0.1
200 PORT command successful.
150 Opening BINARY mode data connection for '126b.fe-0.0.1'.
100% 1476 00:00 ETA
226 Transfer complete.
1476 bytes sent in 0.01 seconds (142.42 KB/s)
```

d. Return to configuration mode.

```
ftp> bye
221 Goodbye.
[edit]
user@host#
```

2. Open the packet capture file on the server with tcpdump or any packet analyzer that supports libpcap format and review the output.

```
root@server% tcpdump -r 126b.fe-0.0.1 -xvvvv

01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl 64, id 33133, offset 0, flags [none], proto: ICMP (1),
length: 84) 14.1.1.1 > 15.1.1.1: ICMP echo request seq 0, length 64
 0005 85c8 f6d1 0005 85c4 e3d1 0800 4500
 0054 816d 0000 4001 da38 0e01 0101 0f01
 0101 0800 3c5a 981e 0000 8b5d 4543 51e6
 0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
 aaaa aaaa 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000
 0000
01:12:36.279793 Out 0:5:85:c8:f6:d1 > 0:5:85:c4:e3:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl 63, id 41227, offset 0, flags [none], proto: ICMP (1),
length: 84) 15.1.1.1 > 14.1.1.1: ICMP echo reply seq 0, length 64
 0005 85c4 e3d1 0005 85c8 f6d1 0800 4500
 0054 a10b 0000 3f01 bb9a 0f01 0101 0e01
 0101 0000 445a 981e 0000 8b5d 4543 51e6
 0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
 aaaa aaaa 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000
 0000
```

```
root@server%
```

#### Related Documentation

- [Packet Capture Overview on page 1927](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Disabling Packet Capture on page 1940](#)
- [Deleting Packet Capture Files on page 1941](#)
- [Disabling Packet Capture on page 1940](#)

## Example: Configuring Packet Capture on an Interface

This example shows how to configure packet capture on an interface to analyze traffic.

- [Requirements on page 1934](#)
- [Overview on page 1934](#)
- [Configuration on page 1934](#)
- [Verification on page 1935](#)

## Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.

## Overview

In this example, you create an interface called fe-0/0/1. You then configure the direction of the traffic for which you are enabling packet capture on the logical interface as inbound and outbound.



**NOTE:** On traffic that bypasses the flow software module (protocol packets such as ARP, OSPF, and PIM), packets generated by the Routing Engine are not captured unless you have configured and applied a firewall filter on the interface in the output direction.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
edit interfaces fe-0/0/1
set unit 0 family inet sampling input output
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#).

To configure packet capture on an interface:

1. Create an interface.

```
[edit]
user@host# edit interfaces fe-0/0/1
```

2. Configure the direction of the traffic.

```
[edit interfaces fe-0/0/1]
user@host# set unit 0 family inet sampling input output
```

3. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

## Verification

### Verifying the Packet Capture Configuration

---

|                              |                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Confirm that the configuration is working properly.                                                |
|                              | Verify that packet capture is configured on the interface.                                         |
| <b>Action</b>                | From configuration mode, enter the <b>show interfaces fe-0/0/1</b> command.                        |
| <b>Related Documentation</b> | • <a href="#">Packet Capture Overview on page 1927</a>                                             |
|                              | • <a href="#">Changing Encapsulation on Interfaces with Packet Capture Configured on page 1941</a> |
|                              | • <a href="#">Example: Configuring a Firewall Filter for Packet Capture on page 1935</a>           |
|                              | • <a href="#">Example: Enabling Packet Capture on a Device on page 1930</a>                        |
|                              | • <a href="#">Deleting Packet Capture Files on page 1941</a>                                       |
|                              | • <a href="#">Disabling Packet Capture on page 1940</a>                                            |

## Example: Configuring a Firewall Filter for Packet Capture

---

This example shows how to configure a firewall filter for packet capture and apply it to a logical interface.

- [Requirements on page 1935](#)
- [Overview on page 1935](#)
- [Configuration on page 1936](#)
- [Verification on page 1937](#)

## Requirements

Before you begin:

- Establish basic connectivity.
- Configure network interfaces. See *Interfaces Feature Guide for Security Devices*.

## Overview

In this example, you set a firewall filter called dest-all and a term name called dest-term to capture packets from a specific destination address, which is 192.168.1.1/32. You define the match condition to accept the sampled packets. Finally, you apply the dest-all filter to all of the outgoing packets on interface fe-0/0/1.



**NOTE:** If you apply a firewall filter on the loopback interface, it affects all traffic to and from the Routing Engine. If the firewall filter has a `sample` action, packets to and from the Routing Engine are sampled. If packet capture is enabled, then packets to and from the Routing Engine are captured in the files created for the input and output interfaces.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set firewall filter dest-all term dest-term from destination-address 192.168.1.1/32
set firewall filter dest-all term dest-term then sample accept
edit interfaces
set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure a firewall filter for packet capture and apply it to a logical interface:

1. Specify the firewall filter and its destination address.

```
[edit]
user@host# edit firewall
user@host# set filter dest-all term dest-term from destination-address 192.168.1.1/32
```

2. Define the match condition and its action.

```
[edit firewall]
user@host# set filter dest-all term dest-term then sample accept
```

3. Apply the filter to all the outgoing packets.

```
[edit interfaces]
user@host# set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

**Results** From configuration mode, confirm your configuration by entering the **show firewall filter dest-all** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show firewall filter dest-all
term dest-term {
 from {
 destination-address 192.168.1.1/32;
 }
 then {
 sample;
 accept;
 }
}
```



```
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying the Firewall Filter for Packet Capture Configuration

**Purpose** Confirm that the configuration is working properly.

Verify that the firewall filter for packet capture is configured.

**Action** From configuration mode, enter the **show firewall filter dest-all** command. Verify that the output shows the intended configuration of the firewall filter for capturing packets sent to the destination address.

#### Related Documentation

- [Packet Capture Overview on page 1927](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Enabling Packet Capture on a Device on page 1930](#)
- [Deleting Packet Capture Files on page 1941](#)
- [Disabling Packet Capture on page 1940](#)

## Example: Configuring Packet Capture for Datapath Debugging

This example shows how to configure packet capture to monitor traffic that passes through the device. Packet capture then dumps the packets into a PCAP file format that can be later examined by the tcpdump utility.

- [Requirements on page 1937](#)
- [Overview on page 1937](#)
- [Configuration on page 1938](#)
- [Verification on page 1939](#)

## Requirements

Before you begin, see “[Debugging the Data Path \(CLI Procedure\)](#)” on page 1894.

## Overview

A filter is defined to filter traffic; then an action profile is applied to the filtered traffic. The action profile specifies a variety of actions on the processing unit. One of the supported actions is packet dump, which sends the packet to the Routing Engine and stores it in proprietary form to be read using the **show security datapath-debug capture** command.

## Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security datapath-debug capture-file my-capture
set security datapath-debug capture-file format pcap
set security datapath-debug capture-file size 1m
set security datapath-debug capture-file files 5
set security datapath-debug maximum-capture-size 400
set security datapath-debug action-profile do-capture event np-ingress packet-dump
set security datapath-debug packet-filter my-filter action-profile do-capture
set security datapath-debug packet-filter my-filter source-prefix 1.2.3.4/32
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [“Using the CLI Editor in Configuration Mode” on page 434](#) in the *CLI User Guide*.

To configure packet capture:

1. Edit the security datapath-debug option for the multiple processing units along the packet-processing path:

```
[edit]
user@host# edit security datapath-debug
```

2. Enable the capture file, the file format, the file size, and the number of files. Size number limits the size of the capture file. After the limit size is reached, if the file number is specified, then the capture file will be rotated to filename *x*, where *x* is auto-incremented until it reaches the specified index and then returns to zero. If no files index is specified, the packets will be discarded after the size limit is reached. The default size is 512 kilobytes.

```
[edit security datapath-debug]
user@host# set capture-file my-capture format pcap size 1m files 5
[edit security datapath-debug]
user@host# set maximum-capture-size 400
```

3. Enable action profile and set the event. Set the action profile as do-capture and the event type as np-ingress:

```
[edit security datapath-debug]
user@host# edit action-profile do-capture
[edit security datapath-debug action-profile do-capture]
user@host# edit event np-ingress
```

4. Enable packet dump for the action profile:

```
[edit security datapath-debug action-profile do-capture event np-ingress]
user@host# set packet-dump
```

5. Enable packet filter, action, and filter options. The packet filter is set to my-filter, the action profile is set to do-capture, and filter option is set to source-prefix 1.2.3.4/32.

```
[edit security datapath-debug]
user@host# set security datapath-debug packet-filter my-filter action-profile
do-capture

[edit security datapath-debug]
user@host# set security datapath-debug packet-filter my-filter source-prefix
1.2.3.4/32
```

**Results** From configuration mode, confirm your configuration by entering the **show security datapath-debug** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it. The following is **show security datapath-debug** output from the **show security datapath-debug** command:

```
security {
 datapath-debug {
 capture-file {
 my-capture
 format pcap
 size 1m
 files 5;
 }
 }
 maximum-capture-size 100;
 action-profile do-capture {
 event np-ingress {
 packet-dump
 }
 }
 packet-filter my-filter {
 source-prefix 1.2.3.4/32
 action-profile do-capture
 }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly.

- [Verifying Packet Capture on page 1939](#)
- [Verifying Data Path Debugging Capture on page 1940](#)
- [Verifying Data Path Debugging Counter on page 1940](#)

### Verifying Packet Capture

**Purpose** Verify if the packet capture is working.

**Action** From operational mode, enter the **request security datapath-debug capture start** command to start packet capture and enter the **request security datapath-debug capture stop** command to stop packet capture.

To view the results, from CLI operational mode, access the local UNIX shell and navigate to the directory `/var/log/my-capture`. The result can be read by using the `tcpdump` utility.

---

### Verifying Data Path Debugging Capture

---

**Purpose** Verify the details of data path debugging capture file.

**Action** From operational mode, enter the `show security datapath-debug capture` command.

```
user@host>show security datapath-debug capture
```



**WARNING:** When you are done troubleshooting, make sure to remove or deactivate all the traceoptions configurations (not limited to flow traceoptions) and the complete security datapath-debug configuration stanza. If any debugging configurations remain active, they will continue to use the device's CPU and memory resources.

---

---

### Verifying Data Path Debugging Counter

---

**Purpose** Verify the details of the data path debugging counter.

**Action** From operational mode, enter the `show security datapath-debug counter` command.

**Related Documentation**

- [Packet Capture Overview on page 1927](#)
- [Understanding Data Path Debugging for SRX Series Devices on page 1893](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1894](#)

---

## Disabling Packet Capture

---

You must disable packet capture before opening the packet capture file for analysis or transferring the file to an external device. Disabling packet capture ensures that the internal file buffer is flushed and all the captured packets are written to the file.

To disable packet capture, enter from configuration mode:

```
[edit forwarding-options]
user@host# set packet-capture disable
```

If you are done configuring the device, enter **commit** from configuration mode.

**Related Documentation**

- [Packet Capture Overview on page 1927](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Example: Enabling Packet Capture on a Device on page 1930](#)

- [Deleting Packet Capture Files on page 1941](#)

## Deleting Packet Capture Files

Deleting packet capture files from the `/var/tmp` directory only temporarily removes the packet capture files. Packet capture files for the interface are automatically created again the next time a packet capture configuration change is committed or as part of a packet capture file rotation.

To delete a packet capture file:

1. Disable packet capture (see [“Disabling Packet Capture” on page 1940](#)).
2. Delete the packet capture file for the interface.
  - a. From operational mode, access the local UNIX shell.
 

```
user@host> start shell
%
```
  - b. Navigate to the directory where packet capture files are stored.
 

```
% cd /var/tmp
%
```
  - c. Delete the packet capture file for the interface; for example `pcap-file.fe.0.0.0`.
 

```
% rm pcap-file.fe.0.0.0
%
```
  - d. Return to operational mode.
 

```
% exit
user@host>
```
3. Reenable packet capture (see [“Example: Enabling Packet Capture on a Device” on page 1930](#)).
4. If you are done configuring the device, enter **commit** from configuration mode.

### Related Documentation

- [Packet Capture Overview on page 1927](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Example: Enabling Packet Capture on a Device on page 1930](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1941](#)
- [Disabling Packet Capture on page 1940](#)

## Changing Encapsulation on Interfaces with Packet Capture Configured

Before modifying the encapsulation on a device interface that is configured for packet capture, you must disable packet capture and rename the latest packet capture file.

Otherwise, packet capture saves the packets with different encapsulations in the same packet capture file. Packet files containing packets with different encapsulations are not useful, because packet analyzer tools like tcpdump cannot analyze such files.

After modifying the encapsulation, you can safely reenabling packet capture on the device.

To change the encapsulation on interfaces with packet capture configured:

1. Disable packet capture (see [“Disabling Packet Capture” on page 1940](#)).
2. Enter **commit** from configuration mode.
3. Rename the latest packet capture file on which you are changing the encapsulation with the **.chdsl** extension.
  - a. From operational mode, access the local UNIX shell.

```
user@host> start shell
%
```
  - b. Navigate to the directory where packet capture files are stored.

```
% cd /var/tmp
%
```
  - c. Rename the latest packet capture file for the interface on which you are changing the encapsulation; for example **fe.0.0.0**.

```
% mv pcap-file.fe.0.0.0 pcap-file.fe.0.0.0.chdsl
%
```
  - d. Return to operational mode.

```
% exit
user@host>
```
4. Change the encapsulation on the interface using the J-Web user interface or CLI configuration editor.
5. If you are done configuring the device, enter **commit** from configuration mode.
6. Reenable packet capture (see [“Example: Enabling Packet Capture on a Device” on page 1930](#)).
7. If you are done configuring the device, enter **commit** from configuration mode.

**Related  
Documentation**

- [Packet Capture Overview on page 1927](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1935](#)
- [Example: Enabling Packet Capture on a Device on page 1930](#)

## Displaying Packet Headers

Enter the **monitor traffic** command to display packet headers transmitted through network interfaces with the following syntax:



**NOTE:** Using the **monitor traffic** command can degrade system performance. We recommend that you use filtering options—such as **count** and **matching**—to minimize the impact to packet throughput on the system.

```
user@host> monitor traffic <absolute-sequence> <count number>
<interface interface-name> <layer2-headers> <matching "expression">
<no-domain-names> <no-promiscuous> <no-resolve> <no-timestamp> <print-ascii>
<print-hex> <size bytes> <brief | detail | extensive>
```

Table 226 describes the **monitor traffic** command options.

**Table 226: CLI monitor traffic Command Options**

| Option                          | Description                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>absolute-sequence</b>        | (Optional) Displays the absolute TCP sequence numbers.                                                                                                                                                                                               |
| <b>count number</b>             | (Optional) Displays the specified number of packet headers. Specify a value from 0 through 100,000. The command quits and exits to the command prompt after this number is reached.                                                                  |
| <b>interface interface-name</b> | (Optional) Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.                                                                                             |
| <b>layer2-headers</b>           | (Optional) Displays the link-layer packet header on each line.                                                                                                                                                                                       |
| <b>matching "expression"</b>    | (Optional) Displays packet headers that match an expression enclosed in quotation marks (" "). Table 227 through Table 229 list match conditions, logical operators, and arithmetic, binary, and relational operators you can use in the expression. |
| <b>no-domain-names</b>          | (Optional) Suppresses the display of the domain name portion of the hostname.                                                                                                                                                                        |
| <b>no-promiscuous</b>           | (Optional) Specifies <i>not</i> to place the monitored interface in promiscuous mode.<br><br>In promiscuous mode, the interface reads every packet that reaches it. In nonpromiscuous mode, the interface reads only the packets addressed to it.    |
| <b>no-resolve</b>               | (Optional) Suppresses the display of hostnames.                                                                                                                                                                                                      |
| <b>no-timestamp</b>             | (Optional) Suppresses the display of packet header timestamps.                                                                                                                                                                                       |
| <b>print-ascii</b>              | (Optional) Displays each packet header in ASCII format.                                                                                                                                                                                              |

Table 226: CLI monitor traffic Command Options (*continued*)

| Option            | Description                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>print-hex</b>  | (Optional) Displays each packet header, except link-layer headers, in hexadecimal format.                                                                                                  |
| <b>size bytes</b> | (Optional) Displays the number of bytes for each packet that you specify. If a packet header exceeds this size, the displayed packet header is truncated. The default value is <b>96</b> . |
| <b>brief</b>      | (Optional) Displays minimum packet header information. This is the default.                                                                                                                |
| <b>detail</b>     | (Optional) Displays packet header information in moderate detail. For some protocols, you must also use the <b>size</b> option to see detailed information.                                |
| <b>extensive</b>  | (Optional) Displays the most extensive level of packet header information. For some protocols, you must also use the <b>size</b> option to see extensive information.                      |

To quit the **monitor traffic** command and return to the command prompt, press Ctrl-C.

To limit the packet header information displayed by the **monitor traffic** command, include the **matching "expression"** option. An expression consists of one or more match conditions listed in [Table 227](#), enclosed in quotation marks ( " "). You can combine match conditions by using the logical operators listed in [Table 228](#) (shown in order of highest to lowest precedence).

For example, to display TCP or UDP packet headers, enter:

```
user@host> monitor traffic matching "tcp || udp"
```

To compare the following types of expressions, use the relational operators listed in [Table 229](#) (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in [Table 229](#).
- Binary—Expressions that use the binary operators listed in [Table 229](#).
- Packet data accessor—Expressions that use the following syntax:

```
protocol [byte-offset <size>]
```

Replace **protocol** with any protocol in [Table 227](#). Replace **byte-offset** with the byte offset, from the beginning of the packet header, to use for the comparison. The optional **size** parameter represents the number of bytes examined in the packet header—1, 2, or 4 bytes.

For example, the following command displays all multicast traffic:

```
user@host> monitor traffic matching "ether[0] & 1 != 0"
```



Table 227: CLI monitor traffic Match Conditions

| Match Condition                                                                       | Description                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Entity Type</b>                                                                    |                                                                                                                                                                                                                                                                          |
| <b>host</b> [ <i>address</i>   <i>hostname</i> ]                                      | Matches packet headers that contain the specified address or hostname. You can prepend any of the following protocol match conditions, followed by a space, to <b>host</b> : <b>arp</b> , <b>ip</b> , <b>rarp</b> , or any of the Directional match conditions.          |
| <b>network</b> <i>address</i>                                                         | Matches packet headers with source or destination addresses containing the specified network address.                                                                                                                                                                    |
| <b>network</b> <i>address</i> mask <i>mask</i>                                        | Matches packet headers containing the specified network address and subnet mask.                                                                                                                                                                                         |
| <b>port</b> [ <i>port-number</i>   <i>port-name</i> ]                                 | Matches packet headers containing the specified source or destination TCP or UDP port number or port name.                                                                                                                                                               |
| <b>Directional</b>                                                                    |                                                                                                                                                                                                                                                                          |
| <b>destination</b>                                                                    | Matches packet headers containing the specified destination. Directional match conditions can be prepended to any Entity Type match conditions, followed by a space.                                                                                                     |
| <b>source</b>                                                                         | Matches packet headers containing the specified source.                                                                                                                                                                                                                  |
| <b>source and destination</b>                                                         | Matches packet headers containing the specified source <i>and</i> destination.                                                                                                                                                                                           |
| <b>source or destination</b>                                                          | Matches packet headers containing the specified source <i>or</i> destination.                                                                                                                                                                                            |
| <b>Packet Length</b>                                                                  |                                                                                                                                                                                                                                                                          |
| <b>less</b> <i>bytes</i>                                                              | Matches packets with lengths less than or equal to the specified value, in bytes.                                                                                                                                                                                        |
| <b>greater</b> <i>bytes</i>                                                           | Matches packets with lengths greater than or equal to the specified value, in bytes.                                                                                                                                                                                     |
| <b>Protocol</b>                                                                       |                                                                                                                                                                                                                                                                          |
| <b>arp</b>                                                                            | Matches all ARP packets.                                                                                                                                                                                                                                                 |
| <b>ether</b>                                                                          | Matches all Ethernet frames.                                                                                                                                                                                                                                             |
| <b>ether</b> [ <b>broadcast</b>   <b>multicast</b> ]                                  | Matches broadcast or multicast Ethernet frames. This match condition can be prepended with <b>source</b> or <b>destination</b> .                                                                                                                                         |
| <b>ether protocol</b> [ <i>address</i>   ( <b>\arp</b>   <b>\ip</b>   <b>\rarp</b> )] | Matches Ethernet frames with the specified address or protocol type. The arguments <b>arp</b> , <b>ip</b> , and <b>rarp</b> are also independent match conditions, so they must be preceded with a backslash (\) when used in the <b>ether protocol</b> match condition. |
| <b>icmp</b>                                                                           | Matches all ICMP packets.                                                                                                                                                                                                                                                |
| <b>ip</b>                                                                             | Matches all IP packets.                                                                                                                                                                                                                                                  |
| <b>ip</b> [ <b>broadcast</b>   <b>multicast</b> ]                                     | Matches broadcast or multicast IP packets.                                                                                                                                                                                                                               |

Table 227: CLI monitor traffic Match Conditions (*continued*)

| Match Condition                                                     | Description                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip protocol</b> [ <i>address</i>   (\icmp   igrp   \tcp   \udp)] | Matches IP packets with the specified address or protocol type. The arguments <b>icmp</b> , <b>tcp</b> , and <b>udp</b> are also independent match conditions, so they must be preceded with a backslash (\) when used in the <b>ip protocol</b> match condition. |
| <b>isis</b>                                                         | Matches all IS-IS routing messages.                                                                                                                                                                                                                               |
| <b>rarp</b>                                                         | Matches all RARP packets.                                                                                                                                                                                                                                         |
| <b>tcp</b>                                                          | Matches all TCP packets.                                                                                                                                                                                                                                          |
| <b>udp</b>                                                          | Matches all UDP packets.                                                                                                                                                                                                                                          |

Table 228: CLI monitor traffic Logical Operators

| Logical Operator  | Description                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>!</b>          | Logical NOT. If the first condition does not match, the next condition is evaluated.                                                                |
| <b>&amp;&amp;</b> | Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped. |
| <b>  </b>         | Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.  |
| <b>()</b>         | Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).        |

Table 229: CLI monitor traffic Arithmetic, Binary, and Relational Operators

| Operator                   | Description           |
|----------------------------|-----------------------|
| <b>Arithmetic Operator</b> |                       |
| <b>+</b>                   | Addition operator.    |
| <b>–</b>                   | Subtraction operator. |
| <b>/</b>                   | Division operator.    |
| <b>Binary Operator</b>     |                       |
| <b>&amp;</b>               | Bitwise AND.          |
| <b>*</b>                   | Bitwise exclusive OR. |
| <b> </b>                   | Bitwise inclusive OR. |

**Table 229: CLI monitor traffic Arithmetic, Binary, and Relational Operators** (*continued*)

| Operator                   | Description                                                                    |
|----------------------------|--------------------------------------------------------------------------------|
| <b>Relational Operator</b> |                                                                                |
| <b>&lt;=</b>               | A match occurs if the first expression is less than or equal to the second.    |
| <b>&gt;=</b>               | A match occurs if the first expression is greater than or equal to the second. |
| <b>&lt;</b>                | A match occurs if the first expression is less than the second.                |
| <b>&gt;</b>                | A match occurs if the first expression is greater than the second.             |
| <b>=</b>                   | A match occurs if the first expression is equal to the second.                 |
| <b>!=</b>                  | A match occurs if the first expression is not equal to the second.             |

The following is sample output from the **monitor traffic** command:

```
user@host> monitor traffic count 4 matching "arp" detail
```

```
Listening on fe-0/0/0, capture size 96 bytes 15:04:16.276780 In arp who-has
193.1.1.1 tell host1.site2.net 15:04:16.376848 In arp who-has host2.site2.net
tell host1.site2.net 15:04:16.376887 In arp who-has 193.1.1.2 tell host1.site2.net
15:04:16.601923 In arp who-has 193.1.1.3 tell host1.site2.net
```

**Related  
Documentation**

- [Packet Capture Overview on page 1927](#)
- [Using the J-Web Packet Capture Tool on page 1947](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1941](#)
- [Example: Configuring Packet Capture on an Interface on page 1933](#)

## Using the J-Web Packet Capture Tool

You can use the J-Web packet capture diagnostic tool when you need to quickly capture and analyze router control traffic on a device. Packet capture on the J-Web user interface allows you to capture traffic destined for, or originating from, the Routing Engine. You can use the J-Web packet capture tool to compose expressions with various matching criteria to specify the packets that you want to capture. You can either choose to decode and view the captured packets in the J-Web user interface as they are captured, or save the captured packets to a file and analyze them offline using packet analyzers such as Ethereal. The J-Web packet capture tool does not capture transient traffic.

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web user interface or CLI configuration editor.

To use J-Web packet capture:

1. Select **Troubleshoot>Packet Capture**.
2. Enter information into the Packet Capture page (see [Table 230](#)). The sample configuration captures the next 10 TCP packets originating from the IP address **10.1.40.48** on port 23 and passing through the Gigabit Ethernet interface **ge-0/0/0**.
3. Save the captured packets to a file, or specify other advanced options by clicking the expand icon next to Advanced options.
4. Click **Start**.

The captured packet headers are decoded and appear in the Packet Capture display.

5. Do one of the following:
  - To stop capturing the packets and stay on the same page while the decoded packet headers are being displayed, click **Stop Capturing**.
  - To stop capturing packets and return to the Packet Capture page, click **OK**.

**Table 230: Packet Capture Field Summary**

| Field        | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Your Action                                                                                                                                                                                                                                                                                         |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface    | <p>Specifies the interface on which the packets are captured.</p> <p>If you select <b>default</b>, packets on the Ethernet management port 0 are captured.</p>                                                                                                                                                                                                                                                                                                                 | Select an interface from the list—for example, <b>ge-0/0/0</b> .                                                                                                                                                                                                                                    |
| Detail level | <p>Specifies the extent of details to be displayed for the packet headers.</p> <ul style="list-style-type: none"> <li>• Brief—Displays the minimum packet header information. This is the default.</li> <li>• Detail—Displays packet header information in moderate detail.</li> <li>• Extensive—Displays the maximum packet header information.</li> </ul>                                                                                                                    | Select <b>Detail</b> from the list.                                                                                                                                                                                                                                                                 |
| Packets      | <p>Specifies the number of packets to be captured. Values range from 1 to <b>1000</b>. Default is <b>10</b>. Packet capture stops capturing packets after this number is reached.</p>                                                                                                                                                                                                                                                                                          | Select the number of packets to be captured from the list—for example, <b>10</b> .                                                                                                                                                                                                                  |
| Addresses    | <p>Specifies the addresses to be matched for capturing the packets using a combination of the following parameters:</p> <ul style="list-style-type: none"> <li>• Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both.</li> <li>• Type—Specifies if packet headers are matched for host address or network address.</li> </ul> <p>You can add multiple entries to refine the match criteria for addresses.</p> | <p>Select address-matching criteria. For example:</p> <ol style="list-style-type: none"> <li>1. From the Direction list, select <b>source</b>.</li> <li>2. From the Type list, select <b>host</b>.</li> <li>3. In the Address box, type <b>10.1.40.48</b>.</li> <li>4. Click <b>Add</b>.</li> </ol> |

Table 230: Packet Capture Field Summary (*continued*)

| Field                   | Function                                                                                                                                                                                                 | Your Action                                                                                                                                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocols               | Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.                                                 | Select a protocol from the list—for example, <b>tcp</b> .                                                                                                                                                                                                                                                                |
| Ports                   | Matches packet headers containing the specified source or destination TCP or UDP port number or port name.                                                                                               | Select a direction and a port. For example:<br><br>1. From the Type list, select <b>src</b> .<br><br>2. In the Port box, type <b>23</b> .                                                                                                                                                                                |
| <b>Advanced Options</b> |                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                          |
| Absolute TCP Sequence   | Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.                                                                                                                 | <ul style="list-style-type: none"> <li>Display absolute TCP sequence numbers in the packet headers by selecting this check box.</li> <li>Stop displaying absolute TCP sequence numbers in the packet headers by clearing this check box.</li> </ul>                                                                      |
| Layer 2 Headers         | Specifies that link-layer packet headers to display.                                                                                                                                                     | <ul style="list-style-type: none"> <li>Include link-layer packet headers while capturing packets, by selecting this check box.</li> <li>Exclude link-layer packet headers while capturing packets by clearing this check box.</li> </ul>                                                                                 |
| Non-Promiscuous         | <p>Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it.</p> <p>In promiscuous mode, the interface reads every packet that reaches it.</p> | <ul style="list-style-type: none"> <li>Read all packets that reach the interface by selecting this check box.</li> <li>Read only packets addressed to the interface by clearing this check box.</li> </ul>                                                                                                               |
| Display Hex             | Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.                                                                                                     | <ul style="list-style-type: none"> <li>Display the packet headers in hexadecimal format by selecting this check box.</li> <li>Stop displaying the packet headers in hexadecimal format by clearing this check box.</li> </ul>                                                                                            |
| Display ASCII and Hex   | Specifies that packet headers are to be displayed in hexadecimal and ASCII format.                                                                                                                       | <ul style="list-style-type: none"> <li>Display the packet headers in ASCII and hexadecimal formats by selecting this check box.</li> <li>Stop displaying the packet headers in ASCII and hexadecimal formats by clearing this check box.</li> </ul>                                                                      |
| Header Expression       | <p>Specifies the match condition for the packets to capture.</p> <p>The match conditions you specify for Addresses, Protocols, and Ports appear in expression format in this field.</p>                  | Enter match conditions in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions. |
| Packet Size             | Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.                      | Type the number of bytes you want to capture for each packet header—for example, <b>256</b> .                                                                                                                                                                                                                            |

Table 230: Packet Capture Field Summary (*continued*)

| Field                     | Function                                                                                                                                                                                                                                                                                      | Your Action                                                                                                                                                                                                                        |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Don't Resolve Addresses   | Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Prevent packet capture from resolving IP addresses to hostnames by selecting this check box.</li> <li>Resolve IP addresses into hostnames by clearing this check box.</li> </ul>            |
| No Timestamp              | Suppresses the display of packet header timestamps.                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>Stop displaying timestamps in the captured packet headers by selecting this check box.</li> <li>Display the timestamp in the captured packet headers by clearing this check box.</li> </ul> |
| Write Packet Capture File | <p>Writes the captured packets to a file in PCAP format in <code>/var/tmp</code>. The files are named with the prefix <code>jweb-pcap</code> and the extension <code>.pcap</code>.</p> <p>If you select this option, the decoded packet headers do not appear on the packet capture page.</p> | <ul style="list-style-type: none"> <li>Save the captured packet headers to a file by selecting this check box.</li> <li>Decode and display the packet headers on the J-Web page by clearing this check box.</li> </ul>             |

#### Related Documentation

- [Packet Capture Overview on page 1927](#)
- [Diagnostic Tools Overview on page 1398](#)
- [J-Web Packet Capture Results and Output Summary on page 1950](#)
- [Using the J-Web Ping MPLS Tool on page 1917](#)
- [Using the J-Web Ping Host Tool on page 1914](#)
- [Using the J-Web Traceroute Tool on page 1902](#)

## J-Web Packet Capture Results and Output Summary

Table 231 summarizes the output in the packet capture display.

Table 231: J-Web Packet Capture Results and Output Summary

| Field                   | Description                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>timestamp</i></b> | <p>Time when the packet was captured. The timestamp <code>00:45:40.823971</code> means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds.</p> <p><b>NOTE:</b> The time displayed is local time.</p> |
| <b><i>direction</i></b> | Direction of the packet. Specifies whether the packet originated from the Routing Engine ( <b>Out</b> ), or was destined for the Routing Engine ( <b>In</b> ).                                             |
| <b><i>protocol</i></b>  | <p>Protocol for the packet.</p> <p>In the sample output, <b>IP</b> indicates the Layer 3 protocol.</p>                                                                                                     |

Table 231: J-Web Packet Capture Results and Output Summary (*continued*)

| Field                      | Description                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>source address</i>      | <p>Hostname, if available, or IP address and the port number of the packet's origin. If the Don't Resolve Addresses check box is selected, only the IP address of the source displays.</p> <p><b>NOTE:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.</p>                       |
| <i>destination address</i> | <p>Hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port appear.</p> <p><b>NOTE:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.</p> |
| <i>protocol</i>            | <p>Protocol for the packet.</p> <p>In the sample output, <b>TCP</b> indicates the Layer 4 protocol.</p>                                                                                                                                                                                                                                               |
| <i>data size</i>           | Size of the packet (in bytes).                                                                                                                                                                                                                                                                                                                        |

- Related Documentation
- [Packet Capture Overview on page 1927](#)
  - [Diagnostic Tools Overview on page 1398](#)
  - [Using the J-Web Packet Capture Tool on page 1947](#)





# Troubleshooting Security Devices

- [Recovering the Root Password for SRX Series Devices on page 1953](#)
- [Troubleshooting DNS Name Resolution in Logical System Security Policies \(Master Administrators Only\) on page 1954](#)
- [Troubleshooting the Link Services Interface on page 1955](#)
- [Troubleshooting Security Policies on page 1964](#)
- [Understanding Log Error Messages for Troubleshooting ISSU-Related Problems on page 1966](#)

## Recovering the Root Password for SRX Series Devices

---

If you forget the root password for an SRX Series device, you can use the password recovery procedure to reset the root password. This procedure also involves disabling the watchdog functionality to allow the system to properly boot into single-user mode (KB article 17565).



**NOTE:** You need console access to recover the root password

To recover the root password for an SRX Series device:

1. Power on the device by pressing the power button on the front panel. Verify that the **POWER** LED on the front panel turns green.

The device's boot sequence on your management device appears on the terminal emulation screen.

2. When the autoboot completes, press the Spacebar a few times to access the bootstrap loader prompt.
3. In operational mode, disable the watchdog functionality and enter **boot -s** to start up the system in single-user mode.

```
loader>boot -s
```

The SRX Series device will start up in single-user mode.

4. Enter **recovery** to start the root password recovery procedure.

System watchdog timer disabled.

Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: **recovery**

5. Enter configuration mode in the CLI.

6. Set the root password.

```
[edit]
user@host# set system root-authentication plain-text-password
```

7. Enter the new root password.

```
New password: juniper1
Retype new password:
```

8. At the second prompt, reenter the new root password.

9. If you are finished configuring the network, commit the configuration.

```
root@host# commit
commit complete
```

10. Exit from configuration mode.

11. Exit from operational mode.

12. Enter **y** to reboot the device.

```
Reboot the system? [y/n] y
```

The start up messages display on the screen.

13. Once again, press the Spacebar a few times to access the bootstrap loader prompt.

14. In operational mode, enable the watchdog functionality and enter **boot** to start up the system.

```
loader>watchdog enable
loader>boot
```

15. The SRX Series device starts up again and prompts you to enter a user name and password. Enter the newly configured password:

```
Wed Jul 12 14:20:21 UTC 2011
Deviceabc (ttyu0)
login: root
Password: juniper1
```

**Related Documentation**

- [System Log Messages](#)

---

## Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)

---

**Problem**    **Description:** The address of a hostname in an address book entry that is used in a security policy might fail to resolve correctly.

**Cause**      Normally, address book entries that contain dynamic hostnames refresh automatically for SRX Series devices. The TTL field associated with a DNS entry indicates the time after

which the entry should be refreshed in the policy cache. Once the TTL value expires, the SRX Series device automatically refreshes the DNS entry for an address book entry.

However, if the SRX Series device is unable to obtain a response from the DNS server (for example, the DNS request or response packet is lost in the network or the DNS server cannot send a response), the address of a hostname in an address book entry might fail to resolve correctly. This can cause traffic to drop as no security policy or session match is found.

**Solution** The master administrator can use the **show security dns-cache** command to display DNS cache information on the SRX Series device. If the DNS cache information needs to be refreshed, the master administrator can use the **clear security dns-cache** command.



**NOTE:** These commands are only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

**Related Documentation**

- [Understanding Logical System Security Policies](#)

## Troubleshooting the Link Services Interface

To solve configuration problems on a link services interface:

- [Determine Which CoS Components Are Applied to the Constituent Links on page 1955](#)
- [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1957](#)
- [Determine If LFI and Load Balancing Are Working Correctly on page 1957](#)
- [Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device on page 1964](#)

### Determine Which CoS Components Are Applied to the Constituent Links

**Problem** **Description:** You are configuring a multilink bundle, but you also have traffic without MLPPP encapsulation passing through constituent links of the multilink bundle. Do you apply all CoS components to the constituent links, or is applying them to the multilink bundle enough?

**Solution** You can apply a scheduler map to the multilink bundle and its constituent links. Although you can apply several CoS components with the scheduler map, configure only the ones that are required. We recommend that you keep the configuration on the constituent links simple to avoid unnecessary delay in transmission.

[Table 232](#) shows the CoS components to be applied on a multilink bundle and its constituent links.

Table 232: CoS Components Applied on Multilink Bundles and Constituent Links

| Cos Component                                                         | Multilink Bundle | Constituent Links | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------|------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classifier                                                            | Yes              | No                | CoS classification takes place on the incoming side of the interface, not on the transmitting side, so no classifiers are needed on constituent links.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Forwarding class                                                      | Yes              | No                | Forwarding class is associated with a queue, and the queue is applied to the interface by a scheduler map. The queue assignment is predetermined on the constituent links. All packets from Q2 of the multilink bundle are assigned to Q2 of the constituent link, and packets from all the other queues are queued to Q0 of the constituent link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Scheduler map                                                         | Yes              | Yes               | <p>Apply scheduler maps on the multilink bundle and the constituent link as follows:</p> <ul style="list-style-type: none"> <li>• Transmit rate—Make sure that the relative order of the transmit rate configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle.</li> <li>• Scheduler priority—Make sure that the relative order of the scheduler priority configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle.</li> <li>• Buffer size—Because all non-LFI packets from the multilink bundle transit on Q0 of the constituent links, make sure that the buffer size on Q0 of the constituent links is large enough.</li> <li>• RED drop profile—Configure a RED drop profile on the multilink bundle only. Configuring the RED drop profile on the constituent links applies a back pressure mechanism that changes the buffer size and introduces variation. Because this behavior might cause fragment drops on the constituent links, make sure to leave the RED drop profile at the default settings on the constituent links.</li> </ul> |
| Shaping rate for a per-unit scheduler or an interface-level scheduler | No               | Yes               | Because per-unit scheduling is applied only at the end point, apply this shaping rate to the constituent links only. Any configuration applied earlier is overwritten by the constituent link configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Transmit-rate exact or queue-level shaping                            | Yes              | No                | The interface-level shaping applied on the constituent links overrides any shaping on the queue. Thus apply transmit-rate exact shaping on the multilink bundle only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Rewrite rules                                                         | Yes              | No                | Rewrite bits are copied from the packet into the fragments automatically during fragmentation. Thus what you configure on the multilink bundle is carried on the fragments to the constituent links.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 232: CoS Components Applied on Multilink Bundles and Constituent Links (*continued*)

| Cos Component         | Multilink Bundle | Constituent Links | Explanation                                                                                                                                                                                                                       |
|-----------------------|------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual channel group | Yes              | No                | Virtual channel groups are identified through firewall filter rules that are applied on packets only before the multilink bundle. Thus you do not need to apply the virtual channel group configuration to the constituent links. |

### Determine What Causes Jitter and Latency on the Multilink Bundle

**Problem** **Description:** To test jitter and latency, you send three streams of IP packets. All packets have the same IP precedence settings. After configuring LFI and CRTP, the latency increased even over a noncongested link. How can you reduce jitter and latency?

**Solution** To reduce jitter and latency, do the following:

1. Make sure that you have configured a shaping rate on each constituent link.
2. Make sure that you have not configured a shaping rate on the link services interface.
3. Make sure that the configured shaping rate value is equal to the physical interface bandwidth.
4. If shaping rates are configured correctly, and jitter still persists, contact the Juniper Networks Technical Assistance Center (JTAC).

### Determine If LFI and Load Balancing Are Working Correctly

**Problem** **Description:** In this case, you have a single network that supports multiple services. The network transmits data and delay-sensitive voice traffic. After configuring MLPPP and LFI, make sure that voice packets are transmitted across the network with very little delay and jitter. How can you find out if voice packets are being treated as LFI packets and load balancing is performed correctly?

**Solution** When LFI is enabled, data (non-LFI) packets are encapsulated with an MLPPP header and fragmented to packets of a specified size. The delay-sensitive, voice (LFI) packets are PPP-encapsulated and interleaved between data packet fragments. Queuing and load balancing are performed differently for LFI and non-LFI packets.

To verify that LFI is performed correctly, determine that packets are fragmented and encapsulated as configured. After you know whether a packet is treated as an LFI packet or a non-LFI packet, you can confirm whether the load balancing is performed correctly.

**Solution Scenario**—Suppose two Juniper Networks devices, R0 and R1, are connected by a multilink bundle `lsq-0/0/0.0` that aggregates two serial links, `se-1/0/0` and `se-1/0/1`. On R0 and R1, MLPPP and LFI are enabled on the link services interface and the fragmentation threshold is set to 128 bytes.

In this example, we used a packet generator to generate voice and data streams. You can use the packet capture feature to capture and analyze the packets on the incoming interface.

The following two data streams were sent on the multilink bundle:

- 100 data packets of 200 bytes (larger than the fragmentation threshold)
- 500 data packets of 60 bytes (smaller than the fragmentation threshold)

The following two voice streams were sent on the multilink bundle:

- 100 voice packets of 200 bytes from source port 100
- 300 voice packets of 200 bytes from source port 200

To confirm that LFI and load balancing are performed correctly:



**NOTE:** Only the significant portions of command output are displayed and described in this example.

1. Verify packet fragmentation. From operational mode, enter the **show interfaces lsq-0/0/0** command to check that large packets are fragmented correctly.

```

user@R0#> show interfaces lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
 Interface index: 136, SNMP ifIndex: 29
 Link-level type: LinkService, MTU: 1504
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps
 Last flapped : 2006-08-01 10:45:13 PDT (2w0d 06:06 ago)
 Input rate : 0 bps (0 pps)
 Output rate : 0 bps (0 pps)

Logical interface lsq-0/0/0.0 (Index 69) (SNMP ifIndex 42)
 Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
 Bandwidth: 16mbps
 Statistics
 Bundle:
 Fragments:
 Input : 0 0 0 0
 Output: 1100 0 118800 0
 Packets:
 Input : 0 0 0 0
 Output: 1000 0 112000 0
 ...
 Protocol inet, MTU: 1500
 Flags: None
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 9.9.9/24, Local: 9.9.9.10

```

**Meaning**—The output shows a summary of packets transiting the device on the multilink bundle. Verify the following information on the multilink bundle:

- The total number of transiting packets = 1000
- The total number of transiting fragments=1100
- The number of data packets that were fragmented =100

The total number of packets sent (600 + 400) on the multilink bundle match the number of transiting packets (1000), indicating that no packets were dropped.

The number of transiting fragments exceeds the number of transiting packets by 100, indicating that 100 large data packets were correctly fragmented.

**Corrective Action**—If the packets are not fragmented correctly, check your fragmentation threshold configuration. Packets smaller than the specified fragmentation threshold are not fragmented.

2. Verify packet encapsulation. To find out whether a packet is treated as an LFI or non-LFI packet, determine its encapsulation type. LFI packets are PPP encapsulated,

and non-LFI packets are encapsulated with both PPP and MLPPP. PPP and MLPPP encapsulations have different overheads resulting in different-sized packets. You can compare packet sizes to determine the encapsulation type.

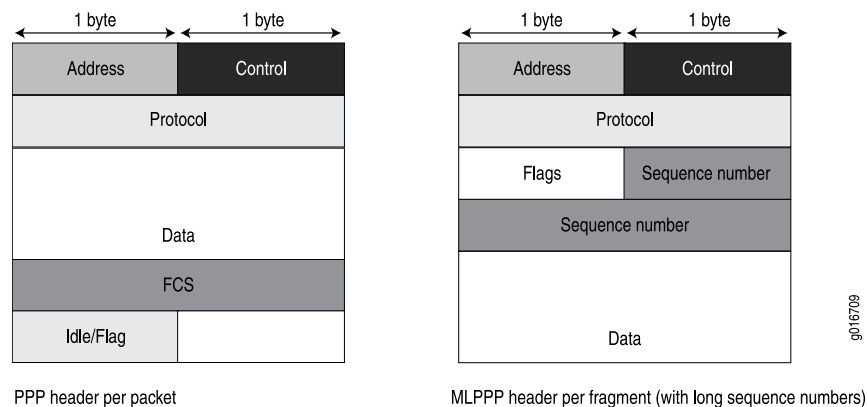
A small unfragmented data packet contains a PPP header and a single MLPPP header. In a large fragmented data packet, the first fragment contains a PPP header and an MLPPP header, but the consecutive fragments contain only an MLPPP header.

PPP and MLPPP encapsulations add the following number of bytes to a packet:

- PPP encapsulation adds 7 bytes:  
4 bytes of header+2 bytes of frame check sequence (FCS)+1 byte that is idle or contains a flag
- MLPPP encapsulation adds between 6 and 8 bytes:  
4 bytes of PPP header+2 to 4 bytes of multilink header

Figure 42 shows the overhead added to PPP and MLPPP headers.

**Figure 42: PPP and MLPPP Headers**



For CRTP packets, the encapsulation overhead and packet size are even smaller than for an LFI packet. For more information, see [Example: Configuring the Compressed Real-Time Transport Protocol](#).

Table 233 shows the encapsulation overhead for a data packet and a voice packet of 70 bytes each. After encapsulation, the size of the data packet is larger than the size of the voice packet.

**Table 233: PPP and MLPPP Encapsulation Overhead**

| Packet Type                                 | Encapsulation | Initial Packet Size | Encapsulation Overhead       | Packet Size after Encapsulation |
|---------------------------------------------|---------------|---------------------|------------------------------|---------------------------------|
| Voice packet (LFI)                          | PPP           | 70 bytes            | 4 + 2 + 1 = 7 bytes          | 77 bytes                        |
| Data fragment (non-LFI) with short sequence | MLPPP         | 70 bytes            | 4 + 2 + 1 + 4 + 2 = 13 bytes | 83 bytes                        |



Table 233: PPP and MLPPP Encapsulation Overhead (*continued*)

| Packet Type                                | Encapsulation | Initial Packet Size | Encapsulation Overhead       | Packet Size after Encapsulation |
|--------------------------------------------|---------------|---------------------|------------------------------|---------------------------------|
| Data fragment (non-LFI) with long sequence | MLPPP         | 70 bytes            | 4 + 2 + 1 + 4 + 4 = 15 bytes | 85 bytes                        |

From operational mode, enter the **show interfaces queue** command to display the size of transmitted packet on each queue. Divide the number of bytes transmitted by the number of packets to obtain the size of the packets and determine the encapsulation type.

3. Verify load balancing. From operational mode, enter the **show interfaces queue** command on the multilink bundle and its constituent links to confirm whether load balancing is performed accordingly on the packets.

```

user@R0> show interfaces queue lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
 Interface index: 136, SNMP ifIndex: 29
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
 Queued:
 Packets : 600 0 pps
 Bytes : 44800 0 bps
 Transmitted:
 Packets : 600 0 pps
 Bytes : 44800 0 bps
 Tail-dropped packets : 0 0 pps
 RED-dropped packets : 0 0 pps
 ...
Queue: 1, Forwarding classes: expedited-forwarding
 Queued:
 Packets : 0 0 pps
 Bytes : 0 0 bps
 ...
Queue: 2, Forwarding classes: VOICE
 Queued:
 Packets : 400 0 pps
 Bytes : 61344 0 bps
 Transmitted:
 Packets : 400 0 pps
 Bytes : 61344 0 bps
 ...
Queue: 3, Forwarding classes: NC
 Queued:
 Packets : 0 0 pps
 Bytes : 0 0 bps
 ...

user@R0> show interfaces queue se-1/0/0
Physical interface: se-1/0/0, Enabled, Physical link is Up
 Interface index: 141, SNMP ifIndex: 35
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
 Queued:

```

```

 Packets : 350 0 pps
 Bytes : 24350 0 bps
 Transmitted:
 Packets : 350 0 pps
 Bytes : 24350 0 bps
 ...
Queue: 1, Forwarding classes: expedited-forwarding
Queued:
 Packets : 0 0 pps
 Bytes : 0 0 bps
...
Queue: 2, Forwarding classes: VOICE
Queued:
 Packets : 100 0 pps
 Bytes : 15272 0 bps
Transmitted:
 Packets : 100 0 pps
 Bytes : 15272 0 bps
...
Queue: 3, Forwarding classes: NC
Queued:
 Packets : 19 0 pps
 Bytes : 247 0 bps
Transmitted:
 Packets : 19 0 pps
 Bytes : 247 0 bps
...

user@R0> show interfaces queue se-1/0/1
Physical interface: se-1/0/1, Enabled, Physical link is Up
 Interface index: 142, SNMP ifIndex: 38
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
Queued:
 Packets : 350 0 pps
 Bytes : 24350 0 bps
Transmitted:
 Packets : 350 0 pps
 Bytes : 24350 0 bps
...
Queue: 1, Forwarding classes: expedited-forwarding
Queued:
 Packets : 0 0 pps
 Bytes : 0 0 bps
...
Queue: 2, Forwarding classes: VOICE
Queued:
 Packets : 300 0 pps
 Bytes : 45672 0 bps
Transmitted:
 Packets : 300 0 pps
 Bytes : 45672 0 bps
...
Queue: 3, Forwarding classes: NC
Queued:
 Packets : 18 0 pps
 Bytes : 234 0 bps
Transmitted:
 Packets : 18 0 pps
 Bytes : 234 0 bps

```

**Meaning**—The output from these commands shows the packets transmitted and queued on each queue of the link services interface and its constituent links. [Table 234](#) shows a summary of these values. (Because the number of transmitted packets equaled the number of queued packets on all the links, this table shows only the queued packets.)

**Table 234: Number of Packets Transmitted on a Queue**

| Packets Queued | Bundle<br>lsq-0/0/0.0 | Constituent Link<br>se-1/0/0 | Constituent Link<br>se-1/0/1 | Explanation                                                                                                                                                          |
|----------------|-----------------------|------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packets on Q0  | 600                   | 350                          | 350                          | The total number of packets transiting the constituent links (350+350 = 700) exceeded the number of packets queued (600) on the multilink bundle.                    |
| Packets on Q2  | 400                   | 100                          | 300                          | The total number of packets transiting the constituent links equaled the number of packets on the bundle.                                                            |
| Packets on Q3  | 0                     | 19                           | 18                           | The packets transiting Q3 of the constituent links are for keepalive messages exchanged between constituent links. Thus no packets were counted on Q3 of the bundle. |

On the multilink bundle, verify the following:

- The number of packets queued matches the number transmitted. If the numbers match, no packets were dropped. If more packets were queued than were transmitted, packets were dropped because the buffer was too small. The buffer size on the constituent links controls congestion at the output stage. To correct this problem, increase the buffer size on the constituent links.
- The number of packets transiting Q0 (600) matches the number of large and small data packets received (100+500) on the multilink bundle. If the numbers match, all data packets correctly transited Q0.
- The number of packets transiting Q2 on the multilink bundle (400) matches the number of voice packets received on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.

On the constituent links, verify the following:

- The total number of packets transiting Q0 (350+350) matches the number of data packets and data fragments (500+200). If the numbers match, all the data packets after fragmentation correctly transited Q0 of the constituent links.

Packets transited both constituent links, indicating that load balancing was correctly performed on non-LFI packets.

- The total number of packets transiting Q2 (300+100) on constituent links matches the number of voice packets received (400) on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.

LFI packets from source port **100** transited **se-1/0/0**, and LFI packets from source port **200** transited **se-1/0/1**. Thus all LFI (Q2) packets were hashed based on the source port and correctly transited both constituent links.

**Corrective Action**—If the packets transited only one link, take the following steps to resolve the problem:

- a. Determine whether the physical link is **up** (operational) or **down** (unavailable). An unavailable link indicates a problem with the PIM, interface port, or physical connection (link-layer errors). If the link is operational, move to the next step.
  - b. Verify that the classifiers are correctly defined for non-LFI packets. Make sure that non-LFI packets are not configured to be queued to Q2. All packets queued to Q2 are treated as LFI packets.
  - c. Verify that at least one of the following values is different in the LFI packets: source address, destination address, IP protocol, source port, or destination port. If the same values are configured for all LFI packets, the packets are all hashed to the same flow and transit the same link.
4. Use the results to verify load balancing.

## Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device

**Problem**    **Description:** You are configuring a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces on a Juniper Networks device and a third-party device, and packets are being dropped and ping fails.

**Solution**    If the third-party device does not have the same FRF.12 support as the Juniper Networks device or supports FRF.12 in a different way, the Juniper Networks device interface on the PVC might discard a fragmented packet containing FRF.12 headers and count it as a "Policed Discard."

As a workaround, configure multilink bundles on both peers, and configure fragmentation thresholds on the multilink bundles.

---

## Troubleshooting Security Policies

- [Checking a Security Policy Commit Failure on page 1964](#)
- [Verifying a Security Policy Commit on page 1965](#)
- [Debugging Policy Lookup on page 1965](#)

### Checking a Security Policy Commit Failure

**Problem**    **Description:** Most policy configuration failures occur during a commit or runtime. Commit failures are reported directly on the CLI when you execute the CLI command **commit-check** in configuration mode. These errors are configuration errors, and you cannot commit the configuration without fixing these errors.

**Solution** To fix these errors, do the following:

1. Review your configuration data.
2. Open the file `/var/log/nsd_chk_only`. This file is overwritten each time you perform a commit check and contains detailed failure information.

## Verifying a Security Policy Commit

**Problem** **Description:** Upon performing a policy configuration commit, if you notice that the system behavior is incorrect, use the following steps to troubleshoot this problem:

- Solution**
1. Operational **show** Commands—Execute the operational commands for security policies and verify that the information shown in the output is consistent with what you expected. If not, the configuration needs to be changed appropriately.
  2. Traceoptions—Set the **traceoptions** command in your policy configuration. The flags under this hierarchy can be selected as per user analysis of the **show** command output. If you cannot determine what flag to use, the flag option **all** can be used to capture all trace logs.

```
user@host# set security policies traceoptions <flag all>
```

You can also configure an optional filename to capture the logs.

```
user@host# set security policies traceoptions <filename>
```

If you specified a filename in the trace options, you can look in the `/var/log/<filename>` for the log file to ascertain if any errors were reported in the file. (If you did not specify a filename, the default filename is `eventd`.) The error messages indicate the place of failure and the appropriate reason.

After configuring the trace options, you must recommit the configuration change that caused the incorrect system behavior.

## Debugging Policy Lookup

**Problem** **Description:** When you have the correct configuration, but some traffic was incorrectly dropped or permitted, you can enable the **lookup** flag in the security policies traceoptions. The **lookup** flag logs the lookup related traces in the trace file.

**Solution** `user@host# set security policies traceoptions <flag lookup>`

- Related Documentation**
- [Synchronizing Policies Between Routing Engine and Packet Forwarding Engine](#)
  - [Checking a Security Policy Commit Failure on page 1964](#)
  - [Verifying a Security Policy Commit on page 1965](#)
  - [Debugging Policy Lookup on page 1965](#)
  - [Monitoring Policy Statistics on page 1819](#)

## Understanding Log Error Messages for Troubleshooting ISSU-Related Problems

---

The following problems might occur during an ISSU upgrade. You can identify the errors by using the details in the logs. You can also see the details of the error messages in the *Junos OS System Log Reference*.

- [Chassisd Process Errors on page 1966](#)
- [Kernel State Synchronization on page 1966](#)
- [Installation Related Errors on page 1966](#)
- [ISSU Support Related Errors on page 1967](#)
- [Redundancy Group Failover Errors on page 1967](#)
- [Initial Validation Checks Fail on page 1967](#)

### Chassisd Process Errors

**Problem**    **Description:** Errors related to chassisd.

**Solution**    Use the error messages to understand the issues related to chassisd.

When ISSU starts, a request is sent to chassisd to check whether there are any problems related to ISSU from a chassis perspective. If there is a problem, a log message is created.

### Kernel State Synchronization

**Problem**    **Description:** Errors related to ksyncd.

**Solution**    Use the following error messages to understand the issues related to ksyncd:

Failed to get kernel-replication error information from Standby Routing Engine.  
mgd\_slave\_peer\_has\_errors() returns error at line 4414 in mgd\_package\_issu.

ISSU checks whether there are any ksyncd errors on the secondary node (node 1) and displays the error message if there are any problems and aborts the ISSU.

### Installation Related Errors

**Problem**    **Description:** The install image file does not exist or the remote site is inaccessible.

**Solution**    Use the following error messages to understand the installation related problems:

error: File does not exist: /var/tmp/junos-srx5000-11.4X3.2-domest  
error: Couldn't retrieve package /var/tmp/junos-srx5000-11.4X3.2-domest

ISSU downloads the install image as specified in the ISSU command as an argument. The image file can be a local file or located at a remote site. If the file does not exist or the remote site is inaccessible, an error is reported.

## ISSU Support Related Errors

**Problem**    **Description:** Installation failure because of unsupported software and unsupported feature configuration.

**Solution**    Use the following error messages to understand the compatibility-related problems:

```
WARNING: Current configuration not compatible with
/var/tmp/junos-srx5000-11.4X3.2-domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
```

## Redundancy Group Failover Errors

**Problem**    **Description:** Problem with automatic redundancy group (RG) failure.

**Solution**    Use the following error messages to understand the problem:

```
failover all RG 1+ groups to node 0
error: Command failed. None of the redundancy-groupss has been failed over.
Some redundancy-groups on node1 are already in manual failover mode.
Please execute 'failover reset all' first..
```

## Initial Validation Checks Fail

**Problem**    **Description:** The initial validation checks fail.

**Solution**    The following error messages are displayed when initial validation checks fail when the image is not present and ISSU is aborted:

### When Image is Not Present

```
user@host> ...0120914_srx_12q1_major2.2-539764-domestic.tgz reboot
Chassis ISSU Started
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade
Initiating in-service-upgrade
Fetching package...
error: File does not exist:
/var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-domestic.tgz
error: Couldn't retrieve package
/var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted
Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.
```

### When Image File is Corrupted

```
user@host> ...junos-srx1k3k-11.4X9-domestic.tgz_1 reboot
```

```
Chassis ISSU Started
node1:

Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade

node1:

Initiating in-service-upgrade
ERROR: Cannot use /var/tmp/junos-srx1k3k-11.4X9-domestic.tgz_1:
gzip: stdin: invalid compressed data--format violated
tar: Child returned status 1
tar: Error exit delayed from previous errors
ERROR: It may have been corrupted during download.
ERROR: Please try again, making sure to use a binary transfer.
Exiting in-service-upgrade window

node1:

Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted

node1:

Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.

{primary:node0}
```

The primary node validates the device configuration to ensure that it can be committed using the new software version. If anything goes wrong, ISSU aborts and error messages are displayed.

**Related  
Documentation**

- [Understanding the Low-Impact ISSU Process on Devices in a Chassis Cluster](#)
- [ISSU System Requirements](#)
- [Upgrading Both Devices in a Chassis Cluster Using an ISSU](#)
- [Troubleshooting Chassis Cluster ISSU-Related Problems](#)



## PART 25

# Configuration Statements and Operational Commands

- [Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options on page 1971](#)
- [Configuration Statements: Chassis Cluster on page 1997](#)
- [Configuration Statements: Datapath Debug on page 2005](#)
- [Configuration Statements: Health Monitoring on page 2015](#)
- [Configuration Statements: Remote Monitoring \(RMON\) on page 2019](#)
- [Configuration Statements: Resource Monitoring for Memory Regions on page 2031](#)
- [Configuration Statements: Security Alarms on page 2041](#)
- [Configuration Statements: SNMP on page 2043](#)
- [Configuration Statements: SNMPv3 on page 2071](#)
- [Operational Commands on page 2115](#)



# Configuration Statements: Accounting Options, Source Class Usage and Destination Class Usage Options

- [accounting-options on page 1972](#)
- [archive-sites on page 1972](#)
- [class-usage-profile on page 1973](#)
- [counters on page 1974](#)
- [destination-classes on page 1974](#)
- [fields \(for Interface Profiles\) on page 1975](#)
- [fields \(for Routing Engine Profiles\) on page 1976](#)
- [file \(Associating with a Profile\) on page 1977](#)
- [file \(Configuring a Log File\) on page 1978](#)
- [files on page 1979](#)
- [filter-profile on page 1980](#)
- [interface-profile on page 1981](#)
- [interval on page 1982](#)
- [mib-profile on page 1983](#)
- [mpls \(Security Forwarding Options\) on page 1984](#)
- [nonpersistent on page 1985](#)
- [object-names on page 1985](#)
- [operation on page 1986](#)
- [packet-capture on page 1987](#)
- [packet-filter on page 1988](#)
- [redundancy-group \(Chassis Cluster\) on page 1989](#)
- [retry-interval \(Chassis Cluster\) on page 1990](#)
- [routing-engine-profile on page 1991](#)
- [size on page 1992](#)
- [source-classes on page 1992](#)

- [start-time](#) on page 1993
- [traceoptions \(System Accounting\)](#) on page 1994
- [transfer-interval](#) on page 1995

## accounting-options

---

|                                 |                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | accounting-options {...}<br>}                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                |
| <b>Description</b>              | Configure options for accounting statistics collection.                                                                                                                                                                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuration Statements at the [edit accounting-options] Hierarchy Level</a> on page 1677</li><li>• <a href="#">Accounting Options Configuration</a> on page 1678</li></ul> |

## archive-sites

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | archive-sites {<br><i>site-name</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format <i>router-name_log-filename_timestamp</i> . |
| <b>Options</b>                  | <i>site-name</i> —Any valid FTP/SCP URL to a destination.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Archive Sites</a> on page 1684</li></ul>                                                                                                                                                                                                                                                                                                                                          |

## class-usage-profile

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>class-usage-profile <i>profile-name</i> {<br/>    file <i>filename</i>;<br/>    interval <i>minutes</i>;<br/>    source-classes {<br/>        <i>source-class-name</i>;<br/>    }<br/>    destination-classes {<br/>        <i>destination-class-name</i>;<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                     |
| Hierarchy Level          | [edit accounting-options]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description              | <p>Create a class usage profile, which is used to log class usage statistics to a file in the <code>/var/log</code> directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has <b>destination-class-usage</b> configured.</p> <p>For information about configuring source classes, see the <a href="#">Junos Routing Protocols Configuration Guide</a>. For information about configuring source class usage, see the <a href="#">Junos Network Management Configuration Guide</a>.</p> |
| Options                  | <p><b>profile-name</b>—Name of the destination class profile.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Class Usage Profiles on page 1695</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## counters

---

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>counters {<br/>    counter-name;<br/>}</pre>                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">filter-profile</a> <i>profile-name</i> ]                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                     |
| <b>Description</b>              | Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the <code>/var/log</code> directory. |
| <b>Options</b>                  | <i>counter-name</i> —Name of the counter.                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Counters on page 1688</a></li></ul>                                                                       |

## destination-classes

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>destination-classes {<br/>    destination-class-name;<br/>}</pre>                                                    |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile</a> <i>profile-name</i> ]                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Specify the destination classes for which statistics are collected.                                                       |
| <b>Options</b>                  | <i>destination-class-name</i> —Name of the destination class to include in the source class usage profile.                |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Class Usage Profile on page 1695</a></li></ul>          |

## fields (for Interface Profiles)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>fields {<br/>    <i>field-name</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit accounting-options <b>interface-profile</b> <i>profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Statistics to collect in an accounting-data log file for an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none"><li>• <b>input-bytes</b>—Input bytes</li><li>• <b>input-errors</b>—Generic input error packets</li><li>• <b>input-multicast</b>—Input packets arriving by multicast</li><li>• <b>input-packets</b>—Input packets</li><li>• <b>input-unicast</b>—Input unicast packets</li><li>• <b>output-bytes</b>—Output bytes</li><li>• <b>output-errors</b>—Generic output error packets</li><li>• <b>output-multicast</b>—Output packets sent by multicast</li><li>• <b>output-packets</b>—Output packets</li><li>• <b>output-unicast</b>—Output unicast packets</li></ul> |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1685</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## fields (for Routing Engine Profiles)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>fields {<br/>    <i>field-name</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit accounting-options <b>routing-engine-profile</b> <i>profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Statistics to collect in an accounting-data log file for a Routing Engine.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none"><li>• <b>cpu-load-1</b>—Average system load over the last 1 minute</li><li>• <b>cpu-load-5</b>—Average system load over the last 5 minutes</li><li>• <b>cpu-load-15</b>—Average system load over the last 15 minutes</li><li>• <b>date</b>—Date, in YYYYMMDD format</li><li>• <b>host-name</b>—Hostname for the router</li><li>• <b>time-of-day</b>—Time of day, in HHMMSS format</li><li>• <b>uptime</b>—Time since last reboot, in seconds</li></ul> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Routing Engine Profile on page 1699</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                |



## file (Associating with a Profile)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file <i>filename</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">filter-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">interface-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">routing-engine-profile <i>profile-name</i></a> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>The [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ] hierarchy added in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series Switches.                                                                                                                                                                               |
| <b>Description</b>              | Specify the accounting log file associated with the profile.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <b><i>filename</i></b> —Name of the log file. You must specify a filename already configured in the <b>file</b> statement at the [edit accounting-options] hierarchy level.                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1685</a></li><li>• <a href="#">Configuring the Filter Profile on page 1687</a></li><li>• <a href="#">Configuring the MIB Profile on page 1697</a></li><li>• <a href="#">Configuring the Routing Engine Profile on page 1699</a></li></ul>                                                                                            |

## file (Configuring a Log File)

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>file <i>filename</i> {<br/>    archive-sites {<br/>        <i>site-name</i>;<br/>    }<br/>    files <i>number</i>;<br/>    nonpersistent;<br/>    size <i>bytes</i>;<br/>    source-classes <i>time</i>;<br/>    transfer-interval <i>minutes</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit accounting-options]                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                            |
| <b>Description</b>              | Specify a log file to be used for accounting data.                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><i>filename</i>—Name of the file in which to write accounting data.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Accounting-Data Log Files on page 1682</a></li></ul>                                                                                                                                                 |

## files

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>files <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                          |
| <b>Description</b>              | Specify the maximum number of log files to be used for accounting data.                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <i>number</i> —The maximum number of files. When a log file (for example, <b>profilelog</b> ) reaches its maximum size, it is renamed <b>profilelog.0</b> , then <b>profilelog.1</b> , and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for <i>number</i> is 3 and the default value is 10. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Accounting-Data Log Files on page 1682</a></li></ul>                                                                                                                                                                                                                                               |

## filter-profile

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>filter-profile <i>profile-name</i> {<br/>    counters {<br/>        counter-name;<br/>    }<br/>    file <i>filename</i>;<br/>    interval <i>minutes</i>;<br/>}</pre>                                                                                                                                                                                                                                                      |
| Hierarchy Level          | [edit accounting-options]                                                                                                                                                                                                                                                                                                                                                                                                        |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                        |
| Description              | Create a profile to filter and collect packet and byte count statistics and write them to a file in the <code>/var/log</code> directory. To apply the profile to a firewall filter, you include the <b>accounting-profile</b> statement at the [edit firewall filter <i>filter-name</i> ] hierarchy level. For more information about firewall filters, see <a href="#">Firewall Filters Feature Guide for Routing Devices</a> . |
| Options                  | <p><i>profile-name</i>—Name of the filter profile.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                 |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                          |
| Related Documentation    | <ul style="list-style-type: none"><li><a href="#">Configuring the Filter Profile on page 1687</a></li></ul>                                                                                                                                                                                                                                                                                                                      |

## interface-profile

---

|                                 |                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface-profile <i>profile-name</i> {<br/>    <b>fields</b> {<br/>        <i>field-name</i>;<br/>    }<br/>    <b>file</b> <i>filename</i>;<br/>    <b>interval</b> <i>minutes</i>;<br/>}</pre>                 |
| <b>Hierarchy Level</b>          | [edit accounting-options]                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                              |
| <b>Description</b>              | Create a profile to filter and collect error and packet statistics and write them to a file in the <code>/var/log</code> directory. You can specify an interface profile for either a physical or a logical interface. |
| <b>Options</b>                  | <p><b><i>profile-name</i></b>—Name of the interface profile.</p> <p>The remaining statements are explained separately.</p>                                                                                             |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1685</a></li></ul>                                                                                                       |

## interval

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interval <i>minutes</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">filter-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">interface-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">routing-engine-profile <i>profile-name</i></a> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>The [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ] hierarchy level added in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                         |
| <b>Description</b>              | Specify how often statistics are collected for the accounting profile.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <b><i>minutes</i></b> —Length of time between each collection of statistics.<br><b>Range:</b> 1 through 2880 minutes<br><b>Default:</b> 30 minutes                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1685</a></li><li>• <a href="#">Configuring the Filter Profile on page 1687</a></li><li>• <a href="#">Configuring the MIB Profile on page 1697</a></li><li>• <a href="#">Configuring the Routing Engine Profile on page 1699</a></li></ul>                                                                                            |

## mib-profile

---

**Syntax**    `mib-profile profile-name {  
                  file filename;  
                  interval minutes;  
                  object-names {  
                      mib-object-name;  
                  }  
                  operation operation-name;  
                  }`

**Hierarchy Level**    [edit accounting-options]

**Release Information**    Statement introduced in Junos OS Release 8.2.  
                              Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**    Create a MIB profile to collect selected MIB statistics and write them to a file in the `/var/log` directory.



**NOTE:** Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

---

**Options**    *profile-name*—Name of the MIB statistics profile.  
  
                  The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring the MIB Profile on page 1697](#)

## mpls (Security Forwarding Options)

---

|                            |                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>mpls {<br/>  mode packet-based;<br/>}</pre>                                  |
| <b>Hierarchy Level</b>     | [edit security forwarding-options family]                                         |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.0.                                     |
| <b>Description</b>         | Enable the forwarding of MPLS traffic. By default, the device drops MPLS traffic. |



**CAUTION:** Because MPLS operates in packet mode, security services are not available.

---



**NOTE:** Packet-based processing is not supported on the following SRX Series devices: SRX1500, SRX5600, and SRX5800.


---

|                                 |                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">MPLS Overview</a></li></ul>                                       |



## nonpersistent

---

|                                 |                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | nonpersistent;                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.                                                                                                                                                                                                                                 |
| <b>Description</b>              | Store log files used for accounting data in the <b>mfs/var/log</b> directory (located on DRAM) instead of the <b>cf/var/log</b> directory (located on the compact flash drive). This feature is useful for minimizing read/write traffic on the router's compact flash drive. |
|                                 | <div> <b>NOTE:</b> If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. Therefore, you should back up these files periodically.</div>       |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Storage Location of the File on page 1682</a></li></ul>                                                                                                                                                   |

## object-names

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | object-names {<br><i>mib-object-name</i> ;<br>}                                                                         |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ]                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.             |
| <b>Options</b>                  | <b><i>mib-object-name</i></b> —Name of a MIB object. You can specify more than one MIB object name.                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the MIB Profile on page 1697</a></li></ul>              |

## operation

---

|                                 |                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>operation operation-name;</code>                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ]                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                          |
| <b>Description</b>              | Specify the name of the operation used to collect MIB statistics for an accounting-data log file.                                                              |
| <b>Options</b>                  | <b><i>operation-name</i></b> —Name of the operation to use. You can specify a <b>get</b> , <b>get-next</b> , or <b>walk</b> operation.<br><b>Default:</b> walk |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the MIB Profile on page 1697</a></li></ul>                                                     |

## packet-capture

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>packet-capture {<br/>  disable;<br/>  file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>bytes</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>  maximum-capture-size <i>number</i>;<br/>}</pre>                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit forwarding-options]                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Configure packet capture on a device.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>disable</b>—Disable packet capture on the router.</p> <p><b>file <i>filename</i></b>—Name of the file to enable packet capture.</p> <ul style="list-style-type: none"><li>• <i>number</i>—Maximum size of file.</li><li>• <i>no-world-readable</i>—Restrict file access to the owner.</li><li>• <i>world-readable</i>—Enable unrestricted file access.</li></ul> <p><b>maximum-capture-size</b>—Configure the maximum size of capture for packets.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Packet Capture Overview on page 1927</a></li></ul>                                                                                                                                                                                                                                                                                                                                                       |

## packet-filter

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>packet-filter <i>packet-filter-name</i> {<br/>    action-profile (<i>profile-name</i>   default);<br/>    destination-port (<i>port-range</i>   <i>protocol-name</i>);<br/>    destination-prefix <i>destination-prefix</i>;<br/>    interface <i>logical-interface-name</i>;<br/>    protocol (<i>protocol-number</i>   <i>protocol-name</i>);<br/>    source-port (<i>port-range</i>   <i>protocol-name</i>);<br/>    source-prefix <i>source-prefix</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit security datapath-debug]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.6 ; Support for IPv6 addresses for the <b>destination-prefix</b> and <b>source-prefix</b> options added in Junos OS Release 10.4. Support for IPv6 filter for the <b>interface</b> option added in Junos OS Release 10.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Set packet filter for taking the datapath-debug action. A maximum of four filters are supported at the same time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b>action-profile</b> (<i>profile-name</i>   default)—Identify the action profile to use. You can specify the name of the action profile to use or select default action profile.</li><li>• <b>destination-port</b> (<i>port-range</i>   <i>protocol name</i>)—Specify a destination port to match TCP/UDP destination port.</li><li>• <b>destination-prefix</b> <i>destination-prefix</i>—Specify a destination IPv4/IPv6 address prefix.</li><li>• <b>interface</b> <i>logical-interface-name</i>—Specify a logical interface name.</li><li>• <b>protocol</b> (<i>protocol-number</i>   <i>protocol-name</i>)—Match IP protocol type.</li><li>• <b>source-port</b> (<i>port-range</i>   <i>protocol-name</i>)—Match TCP/UDP source port.</li><li>• <b>source-prefix</b> <i>source-prefix</i>—Specify a source IP address prefix.</li></ul> |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration<br>security-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## redundancy-group (Chassis Cluster)

**Syntax**

```

redundancy-group group-number {
 gratuitous-arp-count number;
 hold-down-interval number;
 interface-monitor interface-name {
 weight number;
 }
 ip-monitoring {
 family {
 inet {
 ipv4-address {
 interface {
 logical-interface-name;
 secondary-ip-address ip-address;
 }
 weight number;
 }
 }
 }
 global-threshold number;
 global-weight number;
 retry-count number;
 retry-interval seconds;
 }
 node (0 | 1) {
 priority number;
 }
 preempt;
}

```

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Junos OS Release 9.0.

**Description** Define a redundancy group. Except for redundancy group 0, a redundancy group is a logical interface consisting of two physical Ethernet interfaces, one on each chassis. One interface is active, and the other is on standby. When the active interface fails, the standby interface becomes active. The logical interface is called a redundant Ethernet interface (**reth**).

Redundancy group 0 consists of the two Routing Engines in the chassis cluster and controls which Routing Engine is primary. You must define redundancy group 0 in the chassis cluster configuration.

**Options** *group-number* —Redundancy group identification number.

**Range:** 0 through 128



**NOTE:** The maximum number of redundancy groups is equal to the number of redundant Ethernet interfaces that you configure.

The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [ip-monitoring on page 2001](#)

---

## retry-interval (Chassis Cluster)

---

**Syntax** `retry-interval interval;`

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring ]

**Release Information** Statement introduced in Junos OS Release 10.1.

**Description** Specify the ping packet send frequency (in seconds) for each IP address monitored by the redundancy group. (See **retry-count** for a related IP address monitoring configuration variable.)

**Options** *interval*—Pause time between each ping sent to each IP address monitored by the redundancy group.

**Range:** 1 to 30 seconds

**Default:** 1 second

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [ip-monitoring on page 2001](#)

## routing-engine-profile

---

|                                 |                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>routing-engine-profile <i>profile-name</i> {<br/>    <b>fields</b> {<br/>        <i>field-name</i>;<br/>    }<br/>    <b>file</b> <i>filename</i>;<br/>    <b>interval</b> <i>minutes</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit accounting-options]                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                   |
| <b>Description</b>              | Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the <code>/var/log</code> directory.                                                              |
| <b>Options</b>                  | <b><i>profile-name</i></b> —Name of the Routing Engine statistics profile.<br><br>The remaining statements are explained separately.                                                                        |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration.                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Routing Engine Profile on page 1699</a></li></ul>                                                                                       |

## size

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>size bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | Specify attributes of an accounting-data log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <b>bytes</b> —Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, <b>profilelog</b> ) reaches its maximum size, it is renamed <b>profilelog.0</b> , then <b>profilelog.1</b> , and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.<br><br><b>Syntax:</b> <i>x</i> to specify bytes, <i>xk</i> to specify KB, <i>xm</i> to specify MB, <i>xg</i> to specify GB<br><b>Range:</b> 256 KB through 1 GB |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Maximum Size of the File on page 1683</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## source-classes

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>source-classes {<br/>    <i>source-class-name</i>;<br/>}</pre>                                                       |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile</a> <i>profile-name</i> ]                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Specify the source classes for which statistics are collected.                                                            |
| <b>Options</b>                  | <b>source-class-name</b> —Name of the source class to include in the class usage profile.                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Class Usage Profile on page 1695</a></li></ul>          |



## start-time

---

|                                 |                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>start-time <i>time</i>;</code>                                                                                        |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.       |
| <b>Description</b>              | Specify the start time for transfer of an accounting-data log file.                                                         |
| <b>Options</b>                  | <i>time</i> —Start time for file transfer.<br><b>Syntax:</b> <i>YYYY-MM-DD.hh:mm</i>                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Start Time for File Transfer on page 1683</a></li></ul> |

## traceoptions (System Accounting)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   no-world-readable&gt;;     flag (all  config   events   radius   tacplus);     no-remote-trace } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>     | [edit system accounting]]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced in Junos OS Release 14.2.<br><b>tacplus</b> option introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>         | Define tracing operations for System Accounting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Default</b>             | Trace options are not enabled by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—Name of the file in which Junos OS stores the accounting logs. By default, this is created under the /var/log directory.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file reaches the size specified by the size option, the filename is appended with 0 and compressed. For example, when trace file named trace-file-log reaches size &lt;<i>size</i>&gt;, it is renamed and compressed to trace-file-log.0.gz. When trace-file-log reaches size &lt;<i>size</i>&gt; or the second time, the trace-file-log.0.gz is renamed to trace-file-log.1.gz and trace-file-log is renamed and compressed to trace-file-log.0.gz. This renaming scheme ensures that the older logs to have a greater index number. When number of trace files reach &lt;<i>number</i>&gt; then the oldest file is deleted.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option and a filename.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 10</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. You can include one or more of the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations.</li> <li>• <b>config</b>—Trace configuration processing.</li> <li>• <b>events</b>—Trace accounting events and their processing.</li> <li>• <b>radius</b>—Trace RADIUS processing.</li> <li>• <b>tacplus</b>—Trace TACPLUS processing.</li> </ul> <p><b>no-remote-trace</b>—(Optional) Disable tracing and logging operations that track normal operations, error conditions, and packets that are generated by or passed through the Juniper Networks device.</p> <p><b>no-world-readable</b>—Restrict access to the trace files to the owner.</p> |

**Default:** no-world-readable

**size *size***—(Optional) Maximum size of each trace file in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). If you do not specify a unit, the default is bytes. If you specify a maximum file size, you also must specify a maximum number of trace files by using the **files** option and a filename by using the **file** option.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** size to specify bytes, sizek to specify KB, sizem to specify MB, or sizeg to specify GB.

**Range:** 10 KB through 1 MB

**Default:** 128 KB

**world-readable**—Enable any user to access the trace files.

|                           |                                                           |
|---------------------------|-----------------------------------------------------------|
| <b>Required Privilege</b> | admin—To view this statement in the configuration.        |
| <b>Level</b>              | admin-control—To add this statement to the configuration. |

---

## transfer-interval

---

|                              |                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                | transfer-interval <i>minutes</i> ;                                                                                                                                                                          |
| <b>Hierarchy Level</b>       | [edit accounting-options <a href="#">file</a> <i>filename</i> ]                                                                                                                                             |
| <b>Release Information</b>   | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                   |
| <b>Description</b>           | Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.                                                                        |
| <b>Options</b>               | <b><i>minutes</i></b> —Time the file remains open and receives new statistics before it is closed and transferred to an archive site.<br><b>Range:</b> 5 through 2880 minutes<br><b>Default:</b> 30 minutes |
| <b>Required Privilege</b>    | interface—To view this statement in the configuration.                                                                                                                                                      |
| <b>Level</b>                 | interface-control—To add this statement to the configuration.                                                                                                                                               |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Transfer Interval of the File on page 1683</a></li></ul>                                                                                |



## CHAPTER 93

# Configuration Statements: Chassis Cluster

- [cluster \(Chassis\) on page 1998](#)
- [global-threshold on page 1999](#)
- [global-weight on page 2000](#)
- [ip-monitoring on page 2001](#)
- [ip-monitoring \(Services\) on page 2002](#)
- [next-hop on page 2003](#)

## cluster (Chassis)

```

Syntax cluster {
 configuration-synchronize {
 no-secondary-bootup-auto;
 }
 control-link-recovery;
 heartbeat-interval milliseconds;
 heartbeat-threshold number;
 network-management {
 cluster-master;
 }
 redundancy-group group-number {
 gratuitous-arp-count number;
 hold-down-interval number;
 interface-monitor interface-name {
 weight number;
 }
 }
 ip-monitoring {
 family {
 inet {
 ipv4-address {
 interface {
 logical-interface-name;
 secondary-ip-address ip-address;
 }
 weight number;
 }
 }
 }
 global-threshold number;
 global-weight number;
 retry-count number;
 retry-interval seconds;
 }
 node (0 | 1) {
 priority number;
 }
 preempt;
}
reth-count number;
traceoptions {
 file {
 filename;
 files number;
 match regular-expression;
 (world-readable | no-world-readable);
 size maximum-file-size;
 }
 flag flag;
 level {
 (alert | all | critical | debug | emergency | error | info | notice | warning);
 }
 no-remote-trace;
}

```

```

 }
 }

```

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Hierarchy Level</b>          | [edit chassis]                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.0.                                                                           |
| <b>Description</b>              | Configure a chassis cluster.                                                                                            |
| <b>Options</b>                  | The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">ip-monitoring on page 2001</a></li> </ul>                          |

## global-threshold

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | global-threshold <i>number</i> ;                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit chassis cluster redundancy-group <i>group-number</i> ip-monitoring ]                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.1.                                                                                                                                                                                                                       |
| <b>Description</b>              | Specify the failover value for all IP addresses monitored by the redundancy group. When IP addresses with a configured total weight in excess of the threshold have become unreachable, the weight of IP monitoring is deducted from the redundancy group threshold. |
| <b>Options</b>                  | <i>number</i> —Value at which the IP monitoring weight will be applied against the redundancy group failover threshold.<br><b>Range:</b> 0 through 255<br><b>Default:</b> 0                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">ip-monitoring on page 2001</a></li> </ul>                                                                                                                                                                       |

## global-weight

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>global-weight <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit chassis cluster redundancy-group <i>group-number</i> ip-monitoring ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | <p>Specify the relative importance of all IP address monitored objects to the operation of the redundancy group. Every monitored IP address is assigned a weight. If the monitored address becomes unreachable, the weight of the object is deducted from the global-threshold of IP monitoring objects in its redundancy group. When the global-threshold reaches 0, the global-weight is deducted from the redundancy group. Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.</p> |
| <b>Options</b>                  | <p><i>number</i> —Combined weight assigned to all monitored IP addresses. A higher weight value indicates a greater importance.</p> <p><b>Range:</b> 0 through 255</p> <p><b>Default:</b> 255</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">ip-monitoring on page 2001</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## ip-monitoring

```
Syntax ip-monitoring {
 family {
 inet {
 ipv4-address {
 interface {
 logical-interface-name;
 secondary-ip-address ip-address;
 }
 weight number;
 }
 }
 }
 global-threshold number;
 global-weight number;
 retry-count number;
 retry-interval seconds;
 }
```

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ]

**Release Information** Statement updated in Junos OS Release 10.1.

**Description** Specify a global IP address monitoring threshold and weight, and the interval between pings (**retry-interval**) and the number of consecutive ping failures (**retry-count**) permitted before an IP address is considered unreachable for all IP addresses monitored by the redundancy group. Also specify IP addresses, a monitoring weight, a redundant Ethernet interface number, and a secondary IP monitoring ping source for each IP address, for the redundancy group to monitor.

**Options** **family inet *IPv4 address***—The address to be continually monitored for reachability.



**NOTE:** All monitored object failures, including IP monitoring, are deducted from the redundancy group threshold priority. Other monitored objects include interface monitor, SPU monitor, cold-sync monitor, and NPC monitor (on supported platforms).

The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [interface \(Chassis Cluster\)](#)
- [global-threshold on page 1999](#)
- [global-weight on page 2000](#)
- [weight](#)

- [Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring on page 1751](#)

## ip-monitoring (Services)

```
Syntax ip-monitoring {
 policy policy-name {
 match {
 rpm-probe [probe-name];
 }
 no-preempt ;
 then {
 interface interface-name (disable | enable);
 preferred-route {
 route destination-address {
 next hop next-hop;
 preferred-metric metric;
 }
 }
 routing-instances name;
 }
 }
 }
 traceoptions {
 file {
 filename;
 files number;
 match regular-expression;
 size maximum-file-size;
 (world-readable | no-world-readable);
 }
 flag flag;
 no-remote-trace;
 }
}
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Configure IP monitoring.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** services—To view this statement in the configuration.  
services-control—To add this statement to the configuration.

**Related Documentation** • [icmp on page 2012](#)

## next-hop

---

|                                 |                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>next-hop <i>next-hop</i>;</code>                                                                                |
| <b>Hierarchy Level</b>          | <code>[edit services rpm probe <i>owner</i> test <i>test-name</i>]</code>                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4.                                                                        |
| <b>Description</b>              | Specify the next-hop address to which the probe should be sent.                                                       |
| <b>Required Privilege Level</b> | services—To view this statement in the configuration.<br>services-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>probe</i></li></ul>                                                        |



## CHAPTER 94

# Configuration Statements: Datapath Debug

- [action-profile](#) on page 2006
- [capture-file \(Security\)](#) on page 2007
- [datapath-debug](#) on page 2008
- [flow \(Security Flow\)](#) on page 2010
- [icmp](#) on page 2012
- [maximum-capture-size \(Datapath Debug\)](#) on page 2012
- [traceoptions \(Security Datapath Debug\)](#) on page 2013

## action-profile

---

**Syntax**    `action-profile profile-name {  
                  event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress |  
                  pot) {  
                  count;  
                  packet-dump;  
                  packet-summary;  
                  trace;  
                  }  
                  module {  
                  flow {  
                  flag {  
                  all;  
                  }  
                  }  
                  }  
                  }  
                  preserve-trace-order;  
                  record-pic-history;  
                  }`

**Hierarchy Level**    [edit security datapath-debug]

**Release Information**    Command introduced in Junos OS Release 10.0.

**Description**    Configure the action profile options for data path debugging.

- Options**
- ***action-profile name*** — Name of the action profile.
  - **event**—Enable the events to trace the packet when the packet hit the events (jexec, lbt, lt-enter, lt-leave, mac-egress, mac-ingress, np-egress, np-ingress, pot)
    - **count**—Number of times a packet hits the specified event.
    - **packet-dump**—Capture the packet that hits the specified event.
    - **packet-summary**—Print the source/destination IP address details with protocol number and IP length details along with trace message for the specified event.
    - **trace**—Print the standard trace message when the packet hits the specified event.
  - **module**—Turn on the flow session related trace messages.
    - **flow**—Trace flow session related messages.
    - **flag**—Specify which flow message needs to be traced.
    - **all**—Trace all possible flow trace messages.
    - **trace**—Print the standard trace message when the packet hits the specified event.
  - **preserve-trace-order**—Preserve trace order.
  - **record-pic-history**—Record the PICs in which the packet has been processed.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation** • [Example: Configuring Packet Capture for Datapath Debugging on page 1937](#)

## capture-file (Security)

**Syntax** `capture-file {  
    filename;  
    files number;  
    format pcap-format;  
    size maximum-file-size;  
    (world-readable | no-world-readable);  
}`

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Sets packet capture for performing the datapath-debug action.

- Options**
- **filename**—Name of the file to receive the output of the packet capturing operation.
  - **files**—Maximum number of capture files.  
  
If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.  
  
Range: 1 through 10 files
  - **format**—Describes the format of the capture file. The default format file is pcap. You can also set it as private (binary) format.
  - **size**—Describes the size limit of the capture file.  
  
If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.  
  
Range: 10 KB through 100 MB
  - **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation** • [System Log Messages](#)

## datapath-debug

```

Syntax datapath-debug {
 action-profile profile-name {
 event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress
 | pot) {
 count;
 packet-dump;
 packet-summary;
 trace;
 }
 module {
 flow {
 flag {
 all;
 }
 }
 }
 }
 preserve-trace-order;
 record-pic-history;
 }
 capture-file {
 filename;
 files number;
 format pacp-format;
 size maximum-file-size;
 (world-readable | no-world-readable);
 }
 maximum-capture-size value;
 packet-filter packet-filter-name {
 action-profile (profile-name | default);
 destination-port (port-range | protocol-name);
 destination-prefix destination-prefix;
 interface logical-interface-name;
 protocol (protocol-number | protocol-name);
 source-port (port-range | protocol-name);
 source-prefix source-prefix;
 }
 traceoptions {
 file {
 filename;
 files number;
 match regular-expression;
 size maximum-file-size;
 (world-readable | no-world-readable);
 }
 no-remote-trace;
 }
 }

```

**Hierarchy Level** [edit security]

**Release Information** Command introduced in Junos OS Release 10.0.



**Description** Configure the data path debugging options.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

**Related Documentation**

- [Understanding Data Path Debugging for Logical Systems](#)

## flow (Security Flow)

---

```
Syntax flow {
 aging {
 early-ageout seconds;
 high-watermark percent;
 low-watermark percent;
 }
 allow-dns-reply;
 ethernet-switching {
 block-non-ip-all;
 bpdu-vlan-flooding;
 bypass-non-ip-unicast;
 no-packet-flooding {
 no-trace-route;
 }
 }
 force-ip-reassembly;
 ipsec-performance-acceleration;
 load distribution {
 session-affinity ipsec;
 }
 pending-sess-queue-length (high | moderate | normal);
 route-change-timeout seconds;
 syn-flood-protection-mode (syn-cookie | syn-proxy);
 tcp-mss {
 all-tcp mss value;
 gre-in {
 mss value;
 }
 gre-out {
 mss value;
 }
 ipsec-vpn {
 mss value;
 }
 }
 tcp-session {
 fin-invalidate-session;
 no-sequence-check;
 no-syn-check;
 no-syn-check-in-tunnel;
 rst-invalidate-session;
 rst-sequence-check;
 strict-syn-check;
 tcp-initial-timeout seconds;
 time-wait-state {
 (session-ageout | session-timeout seconds);
 }
 }
 traceoptions {
 file {
 filename;
 files number;
 }
 }
 }
```

```

 match regular-expression;
 size maximum-file-size;
 (world-readable | no-world-readable);
 }
 flag flag;
 no-remote-trace;
 packet-filter filter-name {
 destination-port port-identifier;
 destination-prefix address;
 interface interface-name;
 protocol protocol-identifier;
 source-port port-identifier;
 source-prefix address;
 }
 rate-limit messages-per-second;
}

```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Junos OS Release 9.5.

**Description** Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

- Enable or disable DNS replies when there is no matching DNS request.
- Set the initial session-timeout values.

**Options** The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- [Juniper Networks Devices Processing Overview](#)
- [Understanding Session Characteristics for SRX Series Services Gateways](#)
- [Understanding Flow in Logical Systems for SRX Series Devices](#)

## icmp

---

|                                 |                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | icmp{<br>destination-interface <i>interface-name</i> ;<br>}                                                                                    |
| <b>Hierarchy Level</b>          | [edit services rpm probe-server]                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                              |
| <b>Description</b>              | Specify the port information for the ICMP server.<br><br>The remaining statements are explained separately. See <a href="#">CLI Explorer</a> . |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Understanding ICMP Fragment Protection</a></li></ul>                                       |

## maximum-capture-size (Datapath Debug)

---

|                                 |                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | maximum-capture-size <i>maximum-capture-size</i> ;                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit security datapath-debug]                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0.                                                                                                                                                |
| <b>Description</b>              | Specifies maximum packet capture length.                                                                                                                                                      |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b>maximum-capture-size</b> <i>maximum-capture-size</i>—Specify the maximum packet capture length.</li></ul><br><b>Range:</b> 68 through 10,000 bytes |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">System Log Messages</a></li></ul>                                                                                                         |

## traceoptions (Security Datapath Debug)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> traceoptions {   file {     filename;     files number;     match regular-expression;     size maximum-file-size;     (world-readable   no-world-readable);   }   no-remote-trace; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>     | [edit security datapath-debug]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b> | Command introduced in Junos OS Release 9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>         | Sets the trace options for datapath-debug.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>             | <ul style="list-style-type: none"> <li><b>file</b>—Configure the trace file options. <ul style="list-style-type: none"> <li><b>filename</b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>. By default, the name of the file is the name of the process being traced.</li> <li><b>files number</b>—Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed to <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.</li> </ul> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 files</p> <p>Default: 10 files</p> </li> <li><b>match regular-expression</b>—Refine the output to include lines that contain the regular expression.</li> <li><b>size maximum-file-size</b>—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <b>trace-file</b> reaches this size, it is renamed <b>trace-file.0</b>. When the trace-file again reaches its maximum size, <b>trace-file.0</b> is renamed <b>trace-file.1</b> and <b>trace-file</b> is renamed <b>trace-file.0</b>. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</li> </ul> <p>If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and a filename.</p> <p>Syntax: x K to specify KB, x m to specify MB, or x g to specify GB</p> <p>Range: 10 KB through 1 GB</p> <p>Default: 128 KB</p> |

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option
- **no-remote-trace**—Set remote tracing as disabled.

|                           |                                                           |
|---------------------------|-----------------------------------------------------------|
| <b>Required Privilege</b> | trace—To view this statement in the configuration.        |
| <b>Level</b>              | trace-control—To add this statement to the configuration. |

# Configuration Statements: Health Monitoring

- [falling-threshold on page 2015](#)
- [health-monitor on page 2016](#)
- [interval on page 2016](#)
- [rising-threshold on page 2017](#)

## falling-threshold

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>falling-threshold <i>percentage</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit snmp ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.0.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | The lower threshold is expressed as a percentage of the maximum possible value for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the <b>rising-threshold</b> . |
| <b>Options</b>                  | <b><i>percentage</i></b> —The lower threshold for the alarm entry.<br><b>Range:</b> 1 through 100<br><b>Default:</b> 70 percent of the maximum possible value                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 1669</a></li> <li>• <a href="#">rising-threshold on page 2017</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |

## health-monitor

---

|                                 |                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>health-monitor {<br/>    falling-threshold <i>percentage</i>;<br/>    interval <i>seconds</i>;<br/>    rising-threshold <i>percentage</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.0.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                       |
| <b>Description</b>              | Configure health monitoring.<br><br>The remaining statements are explained separately.                                                                      |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Health Monitoring on Devices Running Junos OS on page 1667</a></li></ul>                    |

## interval

---

|                                 |                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interval <i>seconds</i>;</pre>                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp health-monitor]                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.0.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                 |
| <b>Description</b>              | Interval between samples.                                                                                                             |
| <b>Options</b>                  | <b><i>seconds</i></b> —Time between samples, in seconds.<br><b>Range:</b> 1 through 2147483647 seconds<br><b>Default:</b> 300 seconds |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interval on page 1669</a></li></ul>                               |



## rising-threshold

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rising-threshold <i>percentage</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit snmp ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.0.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | The upper threshold is expressed as a percentage of the maximum possible value for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the <b>falling-threshold</b> . |
| <b>Options</b>                  | <b><i>percentage</i></b> —The lower threshold for the alarm entry.<br><b>Range:</b> 1 through 100<br><b>Default:</b> 80 percent of the maximum possible value                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">falling-threshold on page 2015</a></li><li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 1669</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                       |



## CHAPTER 96

# Configuration Statements: Remote Monitoring (RMON)

- [alarm \(SNMP RMON\) on page 2020](#)
- [community on page 2021](#)
- [description on page 2021](#)
- [event on page 2022](#)
- [falling-event-index on page 2022](#)
- [falling-threshold on page 2023](#)
- [falling-threshold-interval on page 2024](#)
- [interval on page 2024](#)
- [request-type on page 2025](#)
- [rising-event-index on page 2026](#)
- [rising-threshold on page 2026](#)
- [rmon on page 2027](#)
- [sample-type on page 2027](#)
- [startup-alarm on page 2028](#)
- [syslog-subtag on page 2028](#)
- [type on page 2029](#)
- [variable on page 2029](#)

## alarm (SNMP RMON)

---

**Syntax**    `alarm index {  
                  description description;  
                  falling-event-index index;  
                  falling-threshold integer;  
                  falling-threshold-interval seconds;  
                  interval seconds;  
                  request-type (get-next-request | get-request | walk-request);  
                  rising-event-index index;  
                  rising-threshold integer;  
                  sample-type (absolute-value | delta-value);  
                  startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);  
                  syslog-subtag syslog-subtag;  
                  variable oid-variable;  
                  }`

**Hierarchy Level**    [edit snmp rmon]

**Release Information**    Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**    Configure RMON alarm entries.

**Options**    *index*—Identifies this alarm entry as an integer.  
  
The remaining statements are explained separately.

**Required Privilege Level**    snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring an Alarm Entry and Its Attributes on page 1626](#)
- [event on page 2022](#)
- *RMON MIB Event, Alarm, Log, and History Control Tables*
- *Monitoring RMON MIB Tables*
- *Understanding RMON*

## community

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>community <i>community-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit snmp rmon event <i>index</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | The trap group that is used when generating a trap (if <b>eventType</b> is configured to send traps). If that trap group has the <b>rmon-alarm</b> trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of <b>eventCommunity</b> ). If nothing is configured, traps are sent to each group with the <b>rmon-alarm</b> category set. |
| <b>Options</b>                  | <b>community-name</b> —Identifies the trap group that is used when generating a trap if the event is configured to send traps.                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1630</a></li> </ul>                                                                                                                                                                                                                                                                                                                                       |

## description

---

|                                 |                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>description <i>description</i>;</code>                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit snmp rmon alarm <i>index</i>],</code><br><code>[edit snmp rmon event <i>index</i>]</code>                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                          |
| <b>Description</b>              | Text description of alarm or event.                                                                                                                                                                |
| <b>Options</b>                  | <b>description</b> —Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").                                                          |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Description on page 1627</a></li> <li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1630</a></li> </ul> |

## event

---

|                                 |                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>event <i>index</i> {<br/>    <b>community</b> <i>community-name</i>;<br/>    <b>description</b> <i>description</i>;<br/>    <b>type</b> <i>type</i>;<br/>}</pre>                 |
| <b>Hierarchy Level</b>          | [edit snmp <b>rmon</b> ]                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                             |
| <b>Description</b>              | Configure RMON event entries.                                                                                                                                                         |
| <b>Options</b>                  | <b>index</b> —Identifier for a specific event entry.<br><br>The remaining statements are explained separately.                                                                        |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1630</a></li><li>• <a href="#">alarm (SNMP RMON) on page 2020</a></li></ul> |

## falling-event-index

---

|                                 |                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>falling-event-index <i>index</i>;</pre>                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit snmp rmon <b>alarm</b> <i>index</i> ]                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                          |
| <b>Description</b>              | The index of the event entry that is used when a falling threshold is crossed. If this value is zero, no event is triggered.                                                                       |
| <b>Options</b>                  | <b>index</b> —Index of the event entry that is used when a falling threshold is crossed.<br><b>Range:</b> 0 through 65,535<br><b>Default:</b> 0                                                    |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Falling Event Index or Rising Event Index on page 1627</a></li><li>• <a href="#">rising-event-index on page 2026</a></li></ul> |

---

## falling-threshold

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>falling-threshold <i>integer</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | The lower threshold for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated startup-alarm value is equal to falling-alarm value or rising-or-falling-alarm value. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the <b>rising-threshold</b> . |
| <b>Options</b>                  | <b>integer</b> —The lower threshold for the alarm entry.<br><b>Range:</b> -2,147,483,648 through 2,147,483,647<br><b>Default:</b> 20 percent less than <b>rising-threshold</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 1627</a></li><li>• <a href="#">rising-threshold on page 2026</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## falling-threshold-interval

---

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>falling-threshold-interval seconds;</code>                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                     |
| <b>Description</b>              | Interval between samples when the rising threshold is crossed. Once the alarm crosses the falling threshold, the regular sampling interval is used.                       |
| <b>Options</b>                  | <b>seconds</b> —Time between samples, in seconds.<br><b>Range:</b> 1 through 2,147,483,647 seconds<br><b>Default:</b> 60 seconds                                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Falling Threshold Interval on page 1628</a></li><li>• <a href="#">interval on page 2024</a></li></ul> |

## interval

---

|                                 |                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interval seconds;</code>                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.        |
| <b>Description</b>              | Interval between samples.                                                                                                        |
| <b>Options</b>                  | <b>seconds</b> —Time between samples, in seconds.<br><b>Range:</b> 1 through 2,147,483,647 seconds<br><b>Default:</b> 60 seconds |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interval on page 1628</a></li></ul>                          |



---

## request-type

---

|                                 |                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request-type (get-next-request   get-request   walk-request);                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                        |
| <b>Description</b>              | Extend monitoring to a specific SNMP object instance ( <b>get-request</b> ), or extend monitoring to all object instances belonging to a MIB branch ( <b>walk-request</b> ), or extend monitoring to the next object instance after the instance specified in the configuration ( <b>get-next-request</b> ). |
| <b>Options</b>                  | <b>get-next-request</b> —Performs an SNMP get next request.<br><br><b>get-request</b> —Performs an SNMP get request.<br><br><b>walk-request</b> —Performs an SNMP walk request.<br><b>Default:</b> walk-request                                                                                              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Request Type on page 1629</a></li><li>• <a href="#">variable on page 2029</a></li></ul>                                                                                                                                                  |

## rising-event-index

---

|                                 |                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rising-event-index <i>index</i>;</code>                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit snmp rmon <a href="#">alarm index</a>]</code>                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                           |
| <b>Description</b>              | Index of the event entry that is used when a rising threshold is crossed. If this value is zero, no event is triggered.                                                                             |
| <b>Options</b>                  | <i>index</i> —Index of the event entry that is used when a rising threshold is crossed.<br><b>Range:</b> 0 through 65,535<br><b>Default:</b> 0                                                      |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Falling Event Index or Rising Event Index on page 1627</a></li><li>• <a href="#">falling-event-index on page 2022</a></li></ul> |

## rising-threshold

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rising-threshold <i>integer</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit snmp rmon <a href="#">alarm index</a>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Upper threshold for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold, and the associated startup alarm value is equal to the falling alarm or rising or falling alarm value. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold. |
| <b>Options</b>                  | <i>integer</i> —The lower threshold for the alarm entry.<br><b>Range:</b> -2,147,483,648 through 2,147,483,647                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 1627</a></li><li>• <a href="#">falling-threshold on page 2023</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## rmon

---

|                                 |                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | rmon { ... }                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.      |
| <b>Description</b>              | Configure Remote Monitoring.                                                                                                   |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring an Alarm Entry and Its Attributes on page 1626</a></li> </ul> |

## sample-type

---

|                                 |                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | sample-type (absolute-value   delta-value);                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm</a> index]                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                      |
| <b>Description</b>              | Method of sampling the selected variable.                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>absolute-value</b>—Actual value of the selected variable is used when comparing against the thresholds.</p> <p><b>delta-value</b>—Difference between samples of the selected variable is used when comparing against the thresholds.</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Sample Type on page 1629</a></li> </ul>                                                                                                                                   |

## startup-alarm

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | startup-alarm (falling-alarm   rising-alarm   rising-or-falling-alarm);                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | The alarm that can be sent upon entry startup.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>falling-alarm</b>—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.</p> <p><b>rising-alarm</b>—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.</p> <p><b>rising-or-falling-alarm</b>—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.</p> <p><b>Default:</b> rising-or-falling-alarm</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Startup Alarm on page 1629</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                             |

## syslog-subtag

---

|                                 |                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | syslog-subtag <i>syslog-subtag</i> ;                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                     |
| <b>Description</b>              | Add a tag to the system log message.                                                                                                                      |
| <b>Options</b>                  | <p><b>syslog-subtag <i>syslog-subtag</i></b>—Tag of not more than 80 uppercase characters to be added to syslog messages.</p> <p><b>Default:</b> None</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the System Log Tag on page 1630</a></li></ul>                                             |

## type

---

|                                 |                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>type type;</code>                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">event index</a> ]                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                  |
| <b>Description</b>              | Type of notification generated when a threshold is crossed.                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>type</b>—Type of notification:</p> <ul style="list-style-type: none"> <li>• <b>log</b>—Add an entry to <b>logTable</b>.</li> <li>• <b>log-and-trap</b>—Send an SNMP trap and make a log entry.</li> <li>• <b>none</b>—No notifications are sent.</li> <li>• <b>snmptrap</b>—Send an SNMP trap.</li> </ul> <p><b>Default:</b> <b>log-and-trap</b></p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1630</a></li> </ul>                                                                                                                                                                                                                             |

## variable

---

|                                 |                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>variable oid-variable;</code>                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit snmp rmon <a href="#">alarm index</a> ]                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                      |
| <b>Description</b>              | Object identifier (OID) of MIB variable to be monitored.                                                                                                                                                       |
| <b>Options</b>                  | <b>oid-variable</b> —OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, 1.3.6.1.2.1.2.1.10.1). Alternatively, use the MIB object name (for example, ifInOctets.1). |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Variable on page 1630</a></li> </ul>                                                                                                      |



# Configuration Statements: Resource Monitoring for Memory Regions

- [\[edit system services resource-monitor\] Hierarchy Level](#) on page 2031
- [free-fw-memory-watermark \(Resource Monitor\)](#) on page 2032
- [free-heap-memory-watermark \(Resource Monitor\)](#) on page 2033
- [free-nh-memory-watermark \(Resource Monitor\)](#) on page 2033
- [high-threshold \(Resource Monitor\)](#) on page 2034
- [no-logging \(Resource Monitor\)](#) on page 2034
- [resource-monitor](#) on page 2035
- [resource-type contiguous-pages \(Resource Monitor\)](#) on page 2036
- [resource-type free-dwords \(Resource Monitor\)](#) on page 2037
- [resource-type free-pages \(Resource Monitor\)](#) on page 2038
- [services \(Resource Monitor\)](#) on page 2039
- [traceoptions \(Resource Monitor\)](#) on page 2040

## [\[edit system services resource-monitor\] Hierarchy Level](#)

---

```
system {
 services {
 resource-monitor {
 high-threshold number;
 free-heap-memory-watermark number;
 free-nh-memory-watermark number;
 free-fw-memory-watermark number;
 no-logging;
 resource-category jtree {
 resource-type contiguous-pages {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-dwords {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-pages {
```

```

 low-watermark number;
 high-watermark number;
 }
}
no-throttle;
no-logging;
high-threshold number;
traceoptions {
 file filename <files number> <match regular-expression> <size maximum-file-size>
 <world-readable | no-world-readable>;
 flag flag;
 no-remote-trace;
}
}
}

```

## free-fw-memory-watermark (Resource Monitor)

|                                 |                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>free-fw-memory-watermark <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor]                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Configure the percentage of free memory space used for firewall or filters to be monitored with a watermark value. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.                                                                                           |
| <b>Options</b>                  | <p><b><i>number</i></b>—Percentage of free memory space used for firewall and filters to be monitored with a watermark value. When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.</p> <p><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                  |



## free-heap-memory-watermark (Resource Monitor)

|                                 |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>free-heap-memory-watermark <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor]                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure the percentage of free memory space used for ukernel or heap (ASIC) memory to be monitored with a watermark value. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.                                                                            |
| <b>Options</b>                  | <p><b><i>number</i></b>—Percentage of free memory space used for ukernel or heap to be monitored with a watermark value. When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.</p> <p><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege Level</b> | <p><b>system</b>—To view this statement in the configuration.</p> <p><b>system-control</b>—To add this statement to the configuration.</p>                                                                                                                                                                                                                               |

## free-nh-memory-watermark (Resource Monitor)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>free-nh-memory-watermark <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor]                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Configure the percentage of free memory space used for next-hops to be monitored with a watermark value. The default value and the configured value of the watermark value for the percentage of free next-hop memory also applies to encapsulation memory. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.                                           |
| <b>Options</b>                  | <p><b><i>number</i></b>—Percentage of free memory space used for next-hops to be monitored with a watermark value. The NH memory watermark is applicable only for encapsulation memory (output WAN static RAM memory). When the configured watermark is exceeded, error logs are triggered. The default watermark values for the percentage of free ukernel or heap memory, next-hop memory, and firewall filter memory are 20.</p> <p><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege Level</b> | <p><b>system</b>—To view this statement in the configuration.</p> <p><b>system-control</b>—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                             |

## high-threshold (Resource Monitor)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | high-threshold <i>number</i> ;                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor]                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Configure the high threshold value, exceeding which warnings or error logs are generated, for all the regions of memory, such as heap or ukernel, next-hop and encapsulation, and firewall filter memory. You can configure the resource-monitoring capability on MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs. |
| <b>Options</b>                  | <i>number</i> —High threshold percentage for memory resource utilization<br><b>Range:</b> 1 through 100                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                          |

## no-logging (Resource Monitor)

---

|                                 |                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-logging;                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor]                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                             |
| <b>Description</b>              | Disable the generation of error log messages when the utilization of memory resources exceeds the threshold or checkpoint levels. By default, messages are written to /var/log/rsmonlog.                                    |
| <b>Options</b>                  | <b>no-logging</b> —Disable the generation of error log messages when the utilization of memory resources exceeds the configured level. By default, error logs are recorded when the resource level utilization is exceeded. |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                           |

## resource-monitor

**Syntax**

```
resource-monitor {
 high-threshold number;
 free-heap-memory-watermark number;
 free-nh-memory-watermark number;
 free-fw-memory-watermark number;
 no-logging;
 no-throttle;
 resource-category jtree {
 resource-type contiguous-pages {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-dwords {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-pages {
 low-watermark number;
 high-watermark number;
 }
 }
 no-throttle;
 no-logging;
 high-threshold number;
 traceoptions {
 file filename <files number> <match regular-expression> <size maximum-file-size>
 <world-readable | no-world-readable>;
 flag flag;
 no-remote-trace;
 }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Junos OS Release 15.1 for MX240, MX480, MX960, MX2010, and MX2020 routers.

**Description** Enable the resource monitoring capability to provision sufficient headroom (memory space limits that are set for the application or virtual router) for monitoring the health and operating efficiency of DPCs and MPCs. You can configure the resource-monitoring capability on MX240, MX480, MX960, MX2010, and MX2020 routers with I-chip-based DPCs and Trio-based FPCs.

**Options** **resource-monitor**—Enable the memory resource monitoring mechanism to avoid the system operations from compromising on the health and traffic-handling stability of the line cards by generating error logs when a specified watermark value for memory regions and threshold value for the jtree memory region are exceeded. A trade-off on the system performance can be detrimental for supporting live traffic and protocols.

The remaining statements are explained separately.

|                           |                                                            |
|---------------------------|------------------------------------------------------------|
| <b>Required Privilege</b> | system—To view this statement in the configuration.        |
| <b>Level</b>              | system-control—To add this statement to the configuration. |

---

## resource-type contiguous-pages (Resource Monitor)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | resource-type contiguous-pages {<br>low-watermark <i>number</i> ;<br>high-watermark <i>number</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>     | [edit system services resource-monitor resource-category jtree]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b> | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>         | Configure the type of resource as contiguous pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. You can monitor the memory utilization of resource types on MX Series routers with DPCs and MPCs.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>             | <p><b>contiguous-pages</b>—Specify that memory resource utilization needs to be monitored for contiguous memory blocks or pages.</p> <p><b>low-watermark <i>number</i></b>—Configure the lower range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the low threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> <p><b>high-watermark <i>number</i></b>—Configure the higher range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the high threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege</b>  | system—To view this statement in the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Level</b>               | system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## resource-type free-dwords (Resource Monitor)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | resource-type free-dwords {<br>low-watermark <i>number</i> ;<br>high-watermark <i>number</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor resource-category jtree]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the type of resource as free or unused memory double words (dwords) for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. You can monitor the memory utilization of resource types on MX Series routers with DPCs and MPCs.                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>free-dwords</b>—Specify that memory resource utilization needs to be monitored for free or empty memory dwords.</p> <p><b>low-watermark <i>number</i></b>—Configure the lower range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the low threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> <p><b>high-watermark <i>number</i></b>—Configure the higher range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the high threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## resource-type free-pages (Resource Monitor)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>resource-type free-pages {<br/>    low-watermark <i>number</i>;<br/>    high-watermark <i>number</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit system services resource-monitor resource-category jtree]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Configure the type of resource as free or unused memory pages for which you want to enable the monitoring mechanism to provide sufficient headroom for ensuring effective system performance and traffic-handling capacity. You can monitor the memory utilization of resource types on MX Series routers with DPCs and MPCs.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>free-pages</b>—Specify that memory resource utilization needs to be monitored for free or empty memory blocks or pages.</p> <p><b>low-watermark <i>number</i></b>—Configure the lower range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the low threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> <p><b>high-watermark <i>number</i></b>—Configure the higher range of the watermark or checkpoint value as a percentage for which the resource type configured needs to be monitored. When the high threshold value is exceeded, error log messages are generated.<br/><b>Range:</b> 1 through 100</p> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## services (Resource Monitor)

```
Syntax services {
 resource-monitor {
 high-threshold number;
 free-heap-memory-watermark number;
 free-nh-memory-watermark number;
 free-fw-memory-watermark number;
 no-logging;
 resource-category jtree {
 resource-type contiguous-pages {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-dwords {
 low-watermark number;
 high-watermark number;
 }
 resource-type free-pages {
 low-watermark number;
 high-watermark number;
 }
 }
 no-throttle;
 no-logging;
 high-threshold number;
 traceoptions {
 file filename <files number> <match regular-expression> <size maximum-file-size>
 <world-readable | no-world-readable>;
 flag flag;
 no-remote-trace;
 }
 }
 }
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.

**Description** Configure the properties for evaluating and tracking the utilization of memory resources, such as ukern memory (heap), next-hop memory, and firewall or filter memory. You can define the characteristics to control the generation of system logging error messages, based on the watermark or checkpoint values that are exceeded for the different memory regions or blocks. Also, you can specify the resource category that you want to monitor and analyze for ensuring system stability, especially the health and operating efficiency of I-chip-based line cards and Trio-based FPCs on MX Series routers.

The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

## tracoptions (Resource Monitor)

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>tracoptions {<br/>    file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;<br/>    &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Hierarchy Level          | [edit system services resource-monitor]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Release Information      | Statement introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Description              | Define tracing operations for the memory resource utilization processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Options                  | <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. All files are placed in the directory <code>/var/log</code>.<br/><b>Default:</b> <code>rmopd</code></p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.<br/><b>Range:</b> 2 through 1000<br/><b>Default:</b> 3 files</p> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files</b> option.<br/><b>Range:</b> 10 KB through 1 GB<br/><b>Default:</b> 128 KB</p> <p><b>world-readable</b>—(Optional) Enable unrestricted file access.</p> <p><b>no-world-readable</b>—(Default) Disable unrestricted file access. This means the log file can be accessed only by the user who configured the tracing operation.</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li></ul> |
| Required Privilege Level | <p><b>trace</b>—To view this statement in the configuration.</p> <p><b>trace-control</b>—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



# Configuration Statements: Security Alarms

- [decryption-failures on page 2041](#)
- [idp \(Security Alarms\) on page 2042](#)

## decryption-failures

---

|                                 |                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | decryption-failures {<br>threshold <i>value</i> ;<br>}                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit security alarms potential-violation]                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                           |
| <b>Description</b>              | Raise a security alarm after exceeding a specified number of decryption failures.                                                                                                                                                        |
| <b>Default</b>                  | Multiple decryption failures do not cause an alarm to be raised.                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>failures</b>—Number of decryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.</p> <p><b>Range:</b> 0 through 1 through 1,000,000,000.</p> <p><b>Default:</b> 1000</p> |
| <b>Required Privilege Level</b> | <p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">IPsec VPN Overview</a></li> </ul>                                                                                                                                                   |

## idp (Security Alarms)

---

|                                 |                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | idp;                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit security alarms potential-violation]                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                        |
| <b>Description</b>              | Configure alarms for IDP attack.                                                                                      |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration. |

# Configuration Statements: SNMP

- [access-list on page 2044](#)
- [agent-address on page 2045](#)
- [alarm-id on page 2046](#)
- [alarm-list-name on page 2047](#)
- [alarm-management on page 2048](#)
- [alarm-state on page 2049](#)
- [authorization on page 2050](#)
- [categories on page 2050](#)
- [client-list on page 2051](#)
- [client-list-name on page 2051](#)
- [clients on page 2052](#)
- [commit-delay on page 2052](#)
- [community \(SNMP\) on page 2053](#)
- [contact \(SNMP\) on page 2054](#)
- [description on page 2054](#)
- [destination-port on page 2055](#)
- [enterprise-oid on page 2055](#)
- [filter-duplicates on page 2056](#)
- [filter-interfaces on page 2056](#)
- [interface \(SNMP\) on page 2057](#)
- [location \(SNMP\) on page 2057](#)
- [logical-system on page 2058](#)
- [logical-system-trap-filter on page 2059](#)
- [name on page 2059](#)
- [nonvolatile on page 2060](#)
- [oid on page 2060](#)
- [proxy \(snmp\) on page 2061](#)
- [routing-instance on page 2062](#)

- [routing-instance-access on page 2063](#)
- [snmp on page 2063](#)
- [source-address on page 2064](#)
- [targets on page 2064](#)
- [traceoptions \(SNMP\) on page 2065](#)
- [trap-group on page 2067](#)
- [trap-options on page 2068](#)
- [version \(SNMP\) on page 2069](#)
- [view \(Associating a MIB View with a Community\) on page 2069](#)
- [view \(Configuring a MIB View\) on page 2070](#)

---

## access-list

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>[edit snmp]   routing-instance-access {     access-list {       <i>routing-instance</i>;       <i>routing-instance</i> restrict;     }   }</pre>                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp routing-instance-access]                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.4.                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Create access lists to control SNMP agents in routing instances from accessing SNMP information. To enable the SNMP agent on a routing instance to access SNMP information, specify the routing instance name. To disable the SNMP agent on a routing instance from accessing SNMP information, include the routing-instance name followed by the <b>restrict</b> keyword. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | • <a href="#">routing-instance-access on page 2063</a>                                                                                                                                                                                                                                                                                                                     |

---

## agent-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | agent-address outgoing-interface;                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp trap-options]                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                              |
| <b>Description</b>              | Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is <b>outgoing-interface</b> , which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.                                                                                        |
| <b>Options</b>                  | <b>outgoing-interface</b> —Value of the agent address of all SNMPv1 traps generated by this router or switch. The <b>outgoing-interface</b> option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.<br><b>Default:</b> disabled (the agent address is not specified in SNMPv1 traps). |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Agent Address for SNMP Traps on page 1490</a></li></ul>                                                                                                                                                                                                            |

## alarm-id

---

**Syntax**    `alarm-id id {  
              alarm-state state {  
                  description alarm-description;  
                  notification-id notification-id-of-alarm;  
                  resource-prefix alarm-resource-prefix;  
                  varbind-index varbind-index-in-alarm-varbind-list;  
                  varbind-subtree alarm-varbind-subtree;  
                  varbind-value alarm-varbind-value;  
              }  
          }`

**Hierarchy Level**    [edit snmp alarm-management alarm-list-name]

**Release Information**    Statement introduced in Junos OS Release 14.1.

**Description**    Specify the identifier of the alarm that you need to configure.  
  
The remaining statement is explained separately.

**Required Privilege Level**    snmp—To view this statement in the configuration.  
                                  snmp-control—To add this statement to the configuration.

**Related Documentation**

- [alarm-list-name on page 2047](#)
- [alarm-management on page 2048](#)
- [alarm-state on page 2049](#)
- *jnxAlarmMib*

## alarm-list-name

**Syntax**    alarm-list-name *list-name* {  
               alarm-id *id* {  
                   alarm-state *state* {  
                       description *alarm-description*;  
                       notification-id *notification-id-of-alarm*;  
                       resource-prefix *alarm-resource-prefix*;  
                       varbind-index *varbind-index-in-alarm-varbind-list*;  
                       varbind-subtree *alarm-varbind-subtree*;  
                       varbind-value *alarm-varbind-value*;  
                   }  
               }  
           }

**Hierarchy Level**    [edit snmp alarm-management]

**Release Information**    Statement introduced in Junos OS Release 14.1.

**Description**    Specify the name of the alarm list that you need to configure.

The remaining statements are explained separately.

**Required Privilege Level**    snmp—To view this statement in the configuration.  
                                   snmp-control—To add this statement to the configuration.

**Related Documentation**

- [alarm-id on page 2046](#)
- [alarm-management on page 2048](#)
- [alarm-state on page 2049](#)
- *jnxAlarmMib*

## alarm-management

```
Syntax alarm-management {
 alarm-list-name list-name {
 alarm-id id {
 alarm-state state {
 description alarm-description;
 notification-id notification-id-of-alarm;
 resource-prefix alarm-resource-prefix;
 varbind-index varbind-index-in-alarm-varbind-list;
 varbind-subtree alarm-varbind-subtree;
 varbind-value alarm-varbind-value;
 }
 }
 }
 }
```

**Hierarchy Level** [edit snmp]

**Release Information** Statement introduced in Junos OS Release 14.1.

**Description** Configure the alarm management system to monitor and report active alarms as well as the history of alarms through the SNMP MIB tables supported by the *Alarm MIB*.



**NOTE:** You cannot configure alarms without notifications. It is mandatory to include the notification identifier in the configuration.

The remaining statements are explained separately.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [alarm-id on page 2046](#)
- [alarm-list-name on page 2047](#)
- [alarm-state on page 2049](#)
- *jnxAlarmMib*



## alarm-state

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>alarm-state state {     description <i>alarm-description</i>;     notification-id <i>notification-id-of-alarm</i>;     resource-prefix <i>alarm-resource-prefix</i>;     varbind-index <i>varbind-index-in-alarm-varbind-list</i>;     varbind-subtree <i>alarm-varbind-subtree</i>;     varbind-value <i>alarm-varbind-value</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit snmp alarm-management alarm-list-name]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Specify the state of the alarm and the other parameters that you need to monitor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>description</b> <i>alarm-description</i>—Include a brief description of the alarm.</p> <p><b>notification-id</b> <i>notification-id-of-alarm</i>—Specify the identifier of the notification associated with the alarm.</p> <p><b>resource-prefix</b> <i>alarm-resource-prefix</i>—Specify the resource prefix of the alarm.</p> <p><b>varbind-index</b> <i>varbind-index-in-alarm-varbind-list</i>—Specify the varbind index in the alarm varbind list.<br/> <b>Range:</b> 0 through 4294967295</p> <p><b>varbind-subtree</b> <i>alarm-varbind-subtree</i>—Specify the subtree of the varbind.</p> <p><b>varbind-value</b> <i>alarm-varbind-value</i>—Specify the varbind value of the alarm.<br/> <b>Range:</b> 0 through 2147483647</p> |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">alarm-id on page 2046</a></li> <li>• <a href="#">alarm-list-name on page 2047</a></li> <li>• <a href="#">alarm-management on page 2048</a></li> <li>• <i>jnxAlarmMib</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## authorization

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>authorization <i>authorization</i>;</code>                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | <code>[edit snmp community <i>community-name</i>]</code>                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                       |
| <b>Description</b>              | Set the access authorization for SNMP <b>Get</b> , <b>GetBulk</b> , <b>GetNext</b> , and <b>Set</b> requests.                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>authorization</i> —Access authorization level: <ul style="list-style-type: none"><li>• <b>read-only</b>—Enable <b>Get</b>, <b>GetNext</b>, and <b>GetBulk</b> requests.</li><li>• <b>read-write</b>—Enable all requests, including <b>Set</b> requests. You must configure a view to enable <b>Set</b> requests.</li></ul> <b>Default:</b> <code>read-only</code> |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Communities on page 1479</a></li></ul>                                                                                                                                                                                                                                                          |

## categories

---

|                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>categories {<br/>    <i>category</i>;<br/>}</code>                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-group <i>group-name</i>]</code>                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                            |
| <b>Description</b>              | Define the types of traps that are sent to the targets of the named trap group.                                                                                                                                                                                      |
| <b>Default</b>                  | If you omit the <b>categories</b> statement, all trap types are included in trap notifications.                                                                                                                                                                      |
| <b>Options</b>                  | <i>category</i> —Name of a trap type: <b>authentication</b> , <b>chassis</b> , <b>configuration</b> , <b>link</b> , <b>remote-operations</b> , <b>rmon-alarm</b> , <b>routing</b> , <b>services</b> , <b>sonet-alarms</b> , <b>startup</b> , or <b>vrrp-events</b> . |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li></ul>                                                                                                                                                          |

## client-list

---

|                                 |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-list <i>client-list-name</i> {<br/>    <i>ip-addresses</i>;<br/>}</code>                                                                                                           |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for QFX Series switches. |
| <b>Description</b>              | Define a list of SNMP clients.                                                                                                                                                                  |
| <b>Options</b>                  | <i>client-list-name</i> —Name of the client list.<br><br><i>ip-addresses</i> —IP addresses of the SNMP clients to be added to the client list,                                                  |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Adding a Group of Clients to an SNMP Community on page 1482</a></li> </ul>                                                                 |

## client-list-name

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-list-name <i>client-list-name</i>;</code>                                                                          |
| <b>Hierarchy Level</b>          | [edit snmp community <i>community-name</i> ]                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.           |
| <b>Description</b>              | Add a client list or prefix list to an SNMP community.                                                                          |
| <b>Options</b>                  | <i>client-list-name</i> —Name of the client list or prefix list.                                                                |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Adding a Group of Clients to an SNMP Community on page 1482</a></li> </ul> |

## clients

---

|                                 |                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>clients {<br/>    address &lt;restrict&gt;;<br/>}</pre>                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit snmp community <i>community-name</i> ]                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                  |
| <b>Description</b>              | Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.                                                                                                                                                                                                     |
| <b>Default</b>                  | If you omit the <b>clients</b> statement, all SNMP clients using this community string are authorized to access the router.                                                                                                                                                                                |
| <b>Options</b>                  | <b>address</b> —Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple <b>address</b> options.<br><br><b>restrict</b> —(Optional) Do not allow the specified SNMP client to access the router. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Communities on page 1479</a></li></ul>                                                                                                                                                                                                |

## commit-delay

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>commit-delay <i>seconds</i>;</pre>                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp nonvolatile]                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Configure the timer for the SNMP <b>Set</b> reply and start of the commit.                                                |
| <b>Options</b>                  | <b>seconds</b> —Delay between an affirmative SNMP <b>Set</b> reply and start of the commit.<br><b>Default:</b> 5 seconds  |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Commit Delay Timer on page 1478</a></li></ul>         |

## community (SNMP)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>community <i>community-name</i> {     authorization <i>authorization</i>;     client-list-name <i>client-list-name</i>;     clients {         address restrict;     }     view <i>view-name</i>; }</pre>                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.</p> <p>The SNMP client application specifies an SNMP community name in <b>Get</b>, <b>GetBulk</b>, <b>GetNext</b>, and <b>Set</b> SNMP requests.</p> |
| <b>Default</b>                  | If you omit the <b>community</b> statement, all SNMP requests are denied.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>community-name</b>—Community string. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Communities on page 1479</a></li> </ul>                                                                                                                                                                                                                                                                                                                |

## contact (SNMP)

---

|                                 |                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>contact <i>contact</i>;</code>                                                                                                       |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                  |
| <b>Description</b>              | Define the value of the MIB II <b>sysContact</b> object, which is the contact person for the managed system.                               |
| <b>Options</b>                  | <b>contact</b> —Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").                              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the System Contact on a Device Running Junos OS on page 1474</a></li></ul> |

## description

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>description <i>description</i>;</code>                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Define the value of the MIB II <b>sysDescription</b> object, which is the description of the system being managed.                                                                             |
| <b>Options</b>                  | <b>description</b> —System description. If the name includes spaces, enclose it in quotation marks (" ").                                                                                      |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the System Description on a Device Running Junos OS on page 1475</a></li></ul>                                                 |

## destination-port

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-port <i>port-number</i>;</code>                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp trap-group]                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Assign a trap port number other than the default.                                                                         |
| <b>Default</b>                  | If you omit this statement, the default port is 162.                                                                      |
| <b>Options</b>                  | <i>port-number</i> —SNMP trap port number.                                                                                |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li> </ul>             |

## enterprise-oid

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>enterprise-oid;</code>                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit snmp <a href="#">trap-options</a> ]                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.0                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Add the <b>snmpTrapEnterprise</b> object, which shows the association between an enterprise-specific trap and the organization that defined the trap, to standard SNMP traps. By default, the <b>snmpTrapEnterprise</b> object is added only to the enterprise-specific traps. When the <b>enterprise-oid</b> statement is included in the configuration, <b>snmpTrapEnterprise</b> is added to all the traps generated from the device. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Trap Options on page 1487</a></li> </ul>                                                                                                                                                                                                                                                                                                                           |

## filter-duplicates

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | filter-duplicates;                                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Filter duplicate <b>Get</b> , <b>GetNext</b> , or <b>GetBulk</b> SNMP requests.                                           |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Filtering Duplicate SNMP Requests on page 1478</a></li></ul>          |

## filter-interfaces

---

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>filter-interfaces {<br/>  interfaces {<br/>    all-internal-interfaces;<br/>    interface 1;<br/>    interface 2;<br/>  }<br/>}</pre>                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.4 for EX Series Switches.                                                                                                                                                                                                         |
| <b>Description</b>              | Filter out information related to specific interfaces from the output of SNMP <b>Get</b> and <b>GetNext</b> requests performed on interface-related MIBs.                                                                                                                    |
| <b>Options</b>                  | <p><b>all-internal-interfaces</b>—Filters out information from SNMP <b>Get</b> and <b>GetNext</b> requests for the specified interfaces.</p> <p><b>interfaces</b>—Specifies the interfaces to filter out from the output of SNMP <b>Get</b> and <b>GetNext</b> requests.</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Filtering Interface Information Out of SNMP Get and GetNext Output on page 1495</a></li></ul>                                                                                                                            |



## interface (SNMP)

---


|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface [ <i>interface-names</i> ];</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit snmp]</code>                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Configure the interfaces on which SNMP requests can be accepted.                                                                                                                                                                                                           |
| <b>Default</b>                  | If you omit this statement, SNMP requests entering the router or switch through any interface are accepted.                                                                                                                                                                |
| <b>Options</b>                  | <i>interface-names</i> —Names of one or more logical interfaces.                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1494</a></li> </ul>                                                                                                                         |

## location (SNMP)

---

|                                 |                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>location <i>location</i>;</code>                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit snmp]</code>                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                      |
| <b>Description</b>              | Define the value of the MIB II <b>sysLocation</b> object, which is the physical location of the managed system.                                |
| <b>Options</b>                  | <i>location</i> —Location of the local system. You must enclose the name within quotation marks (" ").                                         |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the System Location for a Device Running Junos OS on page 1475</a></li> </ul> |

## logical-system

|                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                    | <pre>logical-system <i>logical-system-name</i> {     <i>routing-instance</i> <i>routing-instance-name</i>;     <i>source-address</i> <i>address</i>; }</pre>                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                           | <pre>[edit snmp <i>community</i> <i>community-name</i>], [edit snmp <i>trap-group</i>], [edit snmp <i>trap-options</i>] [edit snmp <i>v3target-address</i> <i>target-address-name</i>]</pre>                                                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                                       | <p>Statement introduced in Junos OS Release 9.3</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                                                            |
| <div>  <p><b>NOTE:</b> The <code>logical-system</code> statement replaces the <code>logical-router</code> statement, and is backward-compatible with Junos OS Release 8.3 and later.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                                                                               | <p>Specify a logical system name for SNMP v1 and v2c clients.</p> <p>Include at the <code>[edit snmp trap-options]</code> hierarchy level to specify a logical-system address as the source address of an SNMP trap.</p> <p>Include at the <code>[edit snmp v3 target-address]</code> hierarchy level to specify a logical-system name as the destination address for an SNMPv3 trap or inform.</p> |
| <b>Options</b>                                                                                                                                                                                                                                                                   | <p><i>logical-system-name</i>—Name of the logical system.</p> <p><i>routing-instance</i> <i>routing-instance-name</i>—Statement to specify a routing instance associated with the logical system.</p>                                                                                                                                                                                               |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                  | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• <a href="#">Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555</a></li> <li>• <a href="#">Configuring the Trap Target Address on page 1522</a></li> </ul>                                                                                                                                                                        |

## logical-system-trap-filter

---

|                                 |                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | logical-system-trap-filter;                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.4.                                                                                 |
| <b>Description</b>              | Restrict the routing instances from receiving traps that are not related to the logical system networks to which they belong. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Trap Support for Routing Instances</i></li></ul>                                   |

## name

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | name <i>name</i> ;                                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Set the system name from the command-line interface.                                                                      |
| <b>Options</b>                  | <i>name</i> —System name override.                                                                                        |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Different System Name on page 1477</a></li></ul>        |

## nonvolatile

---

|                                 |                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>nonvolatile {<br/>    <b>commit-delay</b> <i>seconds</i>;<br/>}</code>                                                                                          |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>The <b>commit-delay</b> statement introduced in Junos OS Release 9.0 for EX Series switches.                     |
| <b>Description</b>              | Configure options for SNMP <b>Set</b> requests.<br><br>The statement is explained separately.                                                                         |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Commit Delay Timer on page 1478</a></li><li>• <a href="#">commit-delay on page 2052</a></li></ul> |

## oid

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>oid <i>object-identifier</i> (exclude   include);</code>                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit snmp view <i>view-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Specify an object identifier (OID) used to represent a subtree of MIB objects.                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <b>exclude</b> —Exclude the subtree of MIB objects represented by the specified OID.<br><br><b>include</b> —Include the subtree of MIB objects represented by the specified OID.<br><br><b>object-identifier</b> —OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring MIB Views on page 1496</a></li></ul>                                                                                                                                                                                                                                                                                                                                      |

## proxy (snmp)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> proxy <i>proxy-name</i>{   device-name <i>device-name</i>;   logical-system <i>logical-system</i> {     routing-instance <i>routing-instance</i>;   }   routing-instance <i>routing-instance</i>;   (version-v1   version-v2c) {     snmp-community <i>community-name</i>;     no-default-comm-to-v3-config;   }   version-v3 {     security-name <i>security-name</i>;     context <i>context-name</i>;   } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>     | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b> | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>         | Configure a device to act as a proxy SNMP agent, and specify a name for the proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>             | <p><b>context <i>context-name</i></b>—Specify the SNMPv3 context name as configured on the device specified at <b>edit snmp proxy <i>proxy-name</i> device-name <i>device-name</i></b>. For more information about this statement, see <a href="#">context</a>.</p> <p><b>device-name <i>device-name</i></b>—Specify the name of the device to be managed through the proxy SNMP agent.</p> <p><b>no-default-comm-to-v3-config</b>—(Optional) Specify whether you have to manually configure the statements at the <b>[edit snmp v3 snmp-community <i>community-name</i>]</b> and <b>[edit snmp v3 vacm]</b> hierarchy levels. If this statement is not included in the configuration, the <b>[edit snmp v3 snmp-community <i>community-name</i>]</b> and <b>[edit snmp v3 vacm]</b> hierarchy level configurations are automatically initialized.</p> <p><b><i>proxy-name</i></b>—Specify the name of the proxy.</p> <p><b>security-name <i>security-name</i></b>—Specify the SNMPv3 security name as configured on the device specified at <b>edit snmp proxy <i>proxy-name</i> device-name <i>device-name</i></b>. For more information about this statement, see <a href="#">security-name</a>.</p> <p><b>snmp-community <i>community-name</i></b>—Specify the name of the SNMP community. The community name you configure should match the <b>snmp-community</b> configuration on the device specified at <b>edit snmp proxy <i>proxy-name</i> device-name <i>device-name</i></b>. For more information about this statement, see <a href="#">snmp-community</a>.</p> <p><b>(version-v1   version-v2c)</b>—Specify the SNMP version, and add the relevant configuration.</p> |

**version-v3**—Add the SNMPv3 configuration.

The remaining statements are explained separately.

|                                 |                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Proxy SNMP Agent on page 1484</a></li></ul> |

---

## routing-instance

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | routing-instance <i>routing-instance-name</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp <b>community</b> <i>community-name</i> ],<br>[edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical-system-name</i> ],<br>[edit snmp <b>trap-group</b> <i>group</i> ]                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Added to the [edit snmp <b>community</b> <i>community-name</i> ] hierarchy level in Junos OS Release 8.4.<br>Added to the [edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical-system-name</i> ] hierarchy level in Junos OS Release 9.1.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                                                                                               |
| <b>Description</b>              | <p>Specify a routing instance for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use this routing instance.</p> <p>If the routing instance is defined within a logical system, include the <b>logical-system</b> <i>logical-system-name</i> statement at the [edit snmp <b>community</b> <i>community-name</i>] hierarchy level and specify the <b>routing-instance</b> statement under the [edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical system-name</i>] hierarchy level.</p> |
| <b>Options</b>                  | <i>routing-instance-name</i> —Name of the routing instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li><li>• <a href="#">Configuring the Source Address for SNMP Traps on page 1488</a></li><li>• <a href="#">Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1555</a></li></ul>                                                                                                                                                                                                                                 |

## routing-instance-access

---

|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | [edit snmp]<br><pre> routing-instance-access {   access-list {     routing-instance;     routing-instance restrict;   } }</pre>                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.4.                                                                                                                                                        |
| <b>Description</b>              | Enable SNMP managers in routing instances other than the default routing instance to access SNMP information. For information about the <b>access-list</b> option, see <a href="#">access-list</a> . |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Enabling SNMP Access over Routing Instances on page 1555</a></li> </ul>                                                                         |

## snmp

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | snmp { ... }                                                                                                              |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Configure SNMP.<br><br>SNMP modules cannot have the slash (/) character or the @ character in the name.                   |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP on a Device Running Junos OS</a></li> </ul>         |

## source-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-address <i>address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-options]</code>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Set the source address of every SNMP trap packet sent by this router to a single address regardless of the outgoing interface. If the source address is not specified, the default is to use the address of the outgoing interface as the source address.                                                                                                                                                                                                 |
| <b>Options</b>                  | <b><i>address</i></b> —Source address of SNMP traps. You can configure the source address of trap packets two ways: <b>lo0</b> or a valid IPv4 address configured on one of the router interfaces. The value <b>lo0</b> indicates that the source address of all SNMP trap packets is set to the lowest loopback address configured at interface <b>lo0</b> .<br><b>Default:</b> Disabled. (The source address is the address of the outgoing interface.) |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Source Address for SNMP Traps on page 1488</a></li></ul>                                                                                                                                                                                                                                                                                                                              |

## targets

---

|                                 |                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>targets {<br/>    <i>address</i>;<br/>}</code>                                                                          |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-group <i>group-name</i>]</code>                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.     |
| <b>Description</b>              | Configure one or more systems to receive SNMP traps.                                                                          |
| <b>Options</b>                  | <b><i>address</i></b> —IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.      |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li></ul>                   |



## tracoptions (SNMP)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>tracoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable       no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>     | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b> | <p>Statement introduced before Junos OS Release 7.4.</p> <p><b>file <i>filename</i></b> option added in Junos OS Release 8.1.</p> <p><b>world-readable   no-world-readable</b> option added in Junos OS Release 8.1.</p> <p><b>match <i>regular-expression</i></b> option added in Junos OS Release 8.1.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>         | <p>The output of the tracing operations is placed into log files in the <b>/var/log</b> directory. Each log file is named after the SNMP agent that generates it. Currently, the following logs are created in the <b>/var/log</b> directory when the <b>tracoptions</b> statement is used:</p> <ul style="list-style-type: none"> <li>• chassisd</li> <li>• craftd</li> <li>• ilmids</li> <li>• mib2d</li> <li>• rmopd</li> <li>• serviced</li> <li>• snmpd</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—By default, the name of the log file that records trace output is the name of the process being traced (for example, <b>mib2d</b> or <b>snmpd</b>). Use this option to specify another name.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, <b>snmpd</b>) reaches its maximum size, it is archived by being renamed to <b>snmpd.0</b>. The previous <b>snmpd.1</b> is renamed to <b>snmpd.2</b>, and so on. The oldest archived file is deleted.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 10 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Log all SNMP events.</li> <li>• <b>general</b>—Log general events.</li> </ul> |

- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **subagent**—Log subagent restarts.
- **timer**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**size *size***—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

**Range:** 10 KB through 1 GB

**Default:** 1000 KB

**world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

|                                 |                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration. |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|

|                              |                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Tracing SNMP Activity on a Device Running Junos OS on page 1585</a></li></ul> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

## trap-group

|                                 |                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> trap-group <i>group-name</i> {     categories {         <i>category</i>;     }     destination-port <i>port-number</i>;     routing-instance <i>instance</i>;     targets {         <i>address</i>;     }     version (all   v1   v2); } </pre>                                    |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p>                                                                |
| <b>Description</b>              | Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent. |
| <b>Options</b>                  | <p><b><i>group-name</i></b>—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").</p> <p>The remaining statements are explained separately.</p>                                                                                                      |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li> </ul>                                                                                                                                                                            |

## trap-options

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>trap-options {<br/>    agent-address outgoing-interface;<br/>    source-address address;<br/>}</pre>                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.</p> <p>The remaining statements are explained separately.</p> |
| <b>Default</b>                  | Disabled                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Options on page 1487</a></li></ul>                                                                                                                                                                                                                                                                      |

## version (SNMP)

---

|                                 |                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>version (all   v1   v2);</code>                                                                                                                    |
| <b>Hierarchy Level</b>          | <code>[edit snmp trap-group <i>group-name</i>]</code>                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                |
| <b>Description</b>              | Specify the version number of SNMP traps.                                                                                                                |
| <b>Default</b>                  | <b>all</b> —Send an SNMPv1 and SNMPv2 trap for every trap condition.                                                                                     |
| <b>Options</b>                  | <b>all</b> —Send an SNMPv1 and SNMPv2 trap for every trap condition.<br><br><b>v1</b> —Send SNMPv1 traps only.<br><br><b>v2</b> —Send SNMPv2 traps only. |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Trap Groups on page 1491</a></li></ul>                                              |


## view (Associating a MIB View with a Community)

---

|                                 |                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>view <i>view-name</i>;</code>                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit snmp community <i>community-name</i>]</code>                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                      |
| <b>Description</b>              | Associate a view with a community. A view represents a group of MIB objects.                                                                                   |
| <b>Options</b>                  | <b><i>view-name</i></b> —Name of the view. You must use a view name already configured in the <b>view</b> statement at the <b>[edit snmp]</b> hierarchy level. |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Communities on page 1479</a></li></ul>                                                    |

## view (Configuring a MIB View)

---

|                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                                                                                                                                                                                                                                          | <pre>view <i>view-name</i> {<br/>    <i>oid object-identifier</i> (include   exclude);<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                               |
| Hierarchy Level                                                                                                                                                                                                                                 | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Release Information                                                                                                                                                                                                                             | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                        |
| Description                                                                                                                                                                                                                                     | Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The <b>view</b> statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the <b>view</b> statement at the <b>[edit snmp community <i>community-name</i>]</b> hierarchy level. |
| <div> <b>NOTE:</b> To remove an OID completely, use the <code>delete view all oid oid-number</code> command but omit the <code>include</code> parameter.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Options                                                                                                                                                                                                                                         | <p><b><i>view-name</i></b>—Name of the view.</p> <p>The remaining statement is explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                         |
| Required Privilege Level                                                                                                                                                                                                                        | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                         |
| Related Documentation                                                                                                                                                                                                                           | <ul style="list-style-type: none"><li>• <a href="#">Configuring MIB Views on page 1496</a></li><li>• <a href="#">Associating MIB Views with an SNMP User Group on page 1514</a></li><li>• <a href="#">community on page 2053</a></li></ul>                                                                                                                                                                                                                                       |

## Configuration Statements: SNMPv3

- [address on page 2072](#)
- [address-mask on page 2073](#)
- [authentication-md5 on page 2073](#)
- [authentication-none on page 2074](#)
- [authentication-password on page 2075](#)
- [authentication-sha on page 2076](#)
- [community-name on page 2077](#)
- [context \(SNMPv3\) on page 2078](#)
- [engine-id on page 2079](#)
- [group \(Configuring Group Name\) on page 2080](#)
- [group \(Defining Access Privileges for an SNMPv3 Group\) on page 2081](#)
- [retry-count on page 2081](#)
- [timeout on page 2082](#)
- [local-engine on page 2083](#)
- [message-processing-model on page 2084](#)
- [notify on page 2085](#)
- [notify-filter \(Applying to the Management Target\) on page 2086](#)
- [notify-filter \(Configuring the Profile Name\) on page 2086](#)
- [notify-view on page 2087](#)
- [oid on page 2087](#)
- [parameters on page 2088](#)
- [port on page 2088](#)
- [privacy-3des on page 2089](#)
- [privacy-aes128 on page 2090](#)
- [privacy-des on page 2091](#)
- [privacy-none on page 2091](#)
- [privacy-password on page 2092](#)
- [read-view on page 2093](#)

- [remote-engine](#) on page 2094
- [routing-instance](#) on page 2095
- [security-level \(Defining Access Privileges\)](#) on page 2096
- [security-level \(Generating SNMP Notifications\)](#) on page 2097
- [security-model \(Access Privileges\)](#) on page 2098
- [security-model \(Group\)](#) on page 2099
- [security-model \(SNMP Notifications\)](#) on page 2099
- [security-name \(Community String\)](#) on page 2100
- [security-name \(Security Group\)](#) on page 2101
- [security-name \(SNMP Notifications\)](#) on page 2102
- [security-to-group](#) on page 2103
- [snmp-community](#) on page 2103
- [tag](#) on page 2104
- [tag-list](#) on page 2104
- [target-address](#) on page 2105
- [target-parameters](#) on page 2106
- [type](#) on page 2107
- [user](#) on page 2107
- [usm](#) on page 2108
- [v3](#) on page 2110
- [vacm](#) on page 2112
- [write-view](#) on page 2113

---

## address

---

|                                 |                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>address <i>address</i>;</code>                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-address <i>target-address-name</i> ]                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Specify the SNMP target address.                                                                                            |
| <b>Options</b>                  | <b><i>address</i></b> —IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Address</a> on page 1523</li></ul>                      |



## address-mask

|                                 |                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>address-mask <i>address-mask</i>;</code>                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 target-address <i>target-address-name</i>]</code>                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 on the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Verify the source addresses for a group of target addresses.                                                                                                                                                                                                              |
| <b>Options</b>                  | <i>address-mask</i> combined with the address defines a range of addresses.                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Address Mask on page 1523</a></li> </ul>                                                                                                                                                             |

## authentication-md5

|                            |                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>authentication-md5 {<br/>    <a href="#">authentication-password</a> <i>authentication-password</i>;<br/>}</code>                                                                        |
| <b>Hierarchy Level</b>     | <code>[edit snmp v3 usm local-engine user <i>username</i>],</code><br><code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i>]</code>                                      |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure MD5 as the authentication type for the SNMPv3 user.                                                                                                                                  |



**NOTE:** You can only configure one authentication type for each SNMPv3 user.

The remaining statement is explained separately.

|                                 |                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring MD5 Authentication on page 1509</a></li> </ul> |

## authentication-none

---

|                            |                                                                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | authentication-none;                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | [edit snmp v3 usm local-engine user <i>username</i> ],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> ]                                                                                                                                          |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>         | Configure that there should be no authentication for the SNMPv3 user.                                                                                                                                                                                                      |



**NOTE:** You can configure only one authentication type for each SNMPv3 user.

---

|                                 |                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring No Authentication on page 1510</a></li></ul>  |

## authentication-password

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>authentication-password <i>authentication-password</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm local-engine user <i>username</i> authentication-md5],<br>[edit snmp v3 usm local-engine user <i>username</i> authentication-sha],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> authentication-md5],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> authentication-sha]                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Configure the password for user authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b><i>authentication-password</i></b>—Password that a user enters. The password is then converted into a key that is used for authentication.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> <li>• The password must be at least eight characters long.</li> <li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li> </ul> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring MD5 Authentication on page 1509</a></li> <li>• <a href="#">Configuring SHA Authentication on page 1509</a></li> </ul>                                                                                                                                                                                                                                                                                                      |

## authentication-sha

---

|                            |                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>authentication-sha {<br/>    authentication-password authentication-password;<br/>}</code>                                                                                               |
| <b>Hierarchy Level</b>     | [edit snmp v3 usm local-engine user <i>username</i> ],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> ]                                                              |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>         | Configure the secure hash algorithm (SHA) as the authentication type for the SNMPv3 user.                                                                                                      |




**NOTE:** You can configure only one authentication type for each SNMPv3 user.

---

The remaining statement is explained separately.

|                                 |                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SHA Authentication on page 1509</a></li></ul> |

## community-name


|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>community-name <i>community-name</i>;</code>                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>[edit snmp v3 snmp-community <i>community-index</i>]</code>                                                                                                                                                                                                                     |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                             |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | The community name defines an SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects. |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>community-name</i> —Community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose it in quotation marks (" ").                                                                                 |
| <div>  <p><b>NOTE:</b> Community names must be unique. You cannot configure the same community name at the <code>[edit snmp community]</code> and <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy levels.</p> <p>The community name at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level is encrypted and not displayed in the command-line interface (CLI).</p> </div> |                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Community on page 1536</a></li> </ul>                                                                                                                                                                     |

## context (SNMPv3)

---

|                                 |                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | context <i>context-name</i> ;                                                                                                  |
| <b>Hierarchy Level</b>          | [edit snmp v3 snmp-community <i>community-index</i> ]                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                              |
| <b>Description</b>              | Specify the SNMPv3 context for access control. A context identifies a collection of information accessible for an SNMP entity. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the SNMPv3 Community on page 1536</a></li></ul>                |

## engine-id

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | engine-id {<br>(local <i>engine-id-suffix</i>   use-default-ip-address   use-mac-address);<br>}                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | [edit snmp]                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.1 for EX Series switches.                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> . You can configure the suffix here. |
| <div>  <p><b>NOTE:</b> SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords are based on the previous engine ID.</p> <p>For the engine ID, we recommend using the MAC address of the management port.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p><b>local <i>engine-id-suffix</i></b>—Explicit setting for the engine ID suffix.</p> <p><b>use-default-ip-address</b>—The engine ID suffix is generated from the default IP address.</p> <p><b>use-mac-address</b>—The SNMP engine identifier is generated from the MAC address of the management interface on the router.</p> <p><b>Default:</b> use-default-ip-address</p>                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Local Engine ID on page 1506</a></li> </ul>                                                                                                                                                                                                                                                                                                                  |

## group (Configuring Group Name)

```
Syntax group group-name {
 (default-context-prefix | context-prefix context-prefix){
 security-model (any | usm | v1 | v2c) {
 security-level (authentication | none | privacy) {
 notify-view view-name;
 read-view view-name;
 write-view view-name;
 }
 }
 }
}
```

**Hierarchy Level** [edit snmp v3 vacm access]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description** Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The **default-context-prefix** statement, when included, adds all the contexts configured on the device to the group, whereas the **context-prefix context-prefix** statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series and OCX Series.) When the context prefix is specified as default (for example, **context-prefix default**), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as **logical system/routing instance**. For example, to specify routing instance ri1 in logical system ls1, include **context-prefix ls1/ri1**.

The remaining statements under this hierarchy are explained separately.

**Options** *group-name*—SNMPv3 group name created for the SNMPv3 group.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Group on page 1513](#)



## group (Defining Access Privileges for an SNMPv3 Group)

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>group group-name;</code>                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm security-to-group security-model (usm   v1   v2c)<br><code>security-name security-name</code> ]                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Define access privileges granted to a group.                                                                                                                                                                                                                               |
| <b>Options</b>                  | <i>group-name</i> —Identifies a collection of SNMP security names that belong to the same access policy SNMP.                                                                                                                                                              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Group on page 1518</a></li> </ul>                                                                                                                                                                     |

## retry-count

---

|                                 |                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>retry-count number;</code>                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit snmp v3 <code>target-address target-address-name</code> ]                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                |
| <b>Description</b>              | Configure the retry count for SNMP informs.                                                                                                                                                                                                                  |
| <b>Options</b>                  | <i>number</i> —Maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.<br><b>Default:</b> 3 times |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Informs on page 1529</a></li> <li>• <a href="#">timeout on page 2082</a></li> </ul>                                                                                                    |

## timeout

---

|                                 |                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>timeout <i>seconds</i>;</code>                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit snmp v3 <a href="#">target-address</a> <i>target-address-name</i> ]                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                 |
| <b>Description</b>              | Configure the timeout period (in seconds) for SNMP informs.                                                                                                                                   |
| <b>Options</b>                  | <b><i>seconds</i></b> —Number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted.<br><b>Default:</b> 15 |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring SNMP Informs on page 1529</a></li><li>• <a href="#">retry-count on page 2081</a></li></ul>                                    |

## local-engine

```
Syntax local-engine {
 user username {
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-none;
 authentication-sha {
 authentication-password authentication-password;
 }
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none {
 privacy-password privacy-password;
 }
 }
 }
```

**Hierarchy Level** [edit snmp v3 [usm](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Configure local engine information for the user-based security model (USM).  
  
The remaining statements are explained separately.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [Creating SNMPv3 Users on page 1507](#)

## message-processing-model

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | message-processing-model (v1   v2c   v3);                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-parameters <i>target-parameter-name</i> parameters]                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the message processing model to be used when generating SNMP notifications.                                                                                                          |
| <b>Options</b>                  | v1—SNMPv1 message process model.<br><br>v2c—SNMPv2c message process model.<br><br>v3—SNMPv3 message process model.                                                                             |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Message Processing Model on page 1527</a></li></ul>                                                                        |

## notify

---

|                                 |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> notify <i>name</i> {     tag <i>tag-name</i>;     type (trap   inform); } </pre>                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit snmp v3]                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p><b>type inform</b> option added in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| <b>Description</b>              | Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b><i>name</i></b>—Name assigned to the notification.</p> <p><b><i>tag-name</i></b>—Notifications are sent to all targets configured with this tag.</p> <p><b><i>type</i></b>—Notification type is <b>trap</b> or <b>inform</b>. Traps are unconfirmed notifications. Informs are confirmed notifications.</p>                                             |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Inform Notification Type and Target Address on page 1534</a></li> <li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1520</a></li> </ul>                                                                                                                                 |

## notify-filter (Applying to the Management Target)

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>notify-filter <i>profile-name</i>;</code>                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 <a href="#">target-parameters</a> <i>target-parameters-name</i>]</code>                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Specify the notify filter to be used by a specific set of target parameters.                                                                                                                                                                                               |
| <b>Options</b>                  | <i>profile-name</i> —Name of the notify filter to apply to notifications.                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Applying the Trap Notification Filter on page 1527</a></li></ul>                                                                                                                                                       |

## notify-filter (Configuring the Profile Name)

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>notify-filter <i>profile-name</i> {<br/>    <a href="#">oid</a> <i>oid</i> (include   exclude);<br/>}</code>                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3]</code>                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Specify a group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.                                                                                                                   |
| <b>Options</b>                  | <i>profile-name</i> —Name assigned to the notify filter.<br><br>The remaining statement is explained separately.                                                                                                                                                           |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Trap Notification Filter on page 1522</a></li><li>• <a href="#">oid on page 2087</a></li></ul>                                                                                                         |

## notify-view

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>notify-view <i>view-name</i>;</code>                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i>) security-model (any   usm   v1   v2c) security-level (authentication   none   privacy)]</code>                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).                                                                                                                                                           |
| <b>Options</b>                  | <b><i>view-name</i></b> —Name of the view to which the SNMP user group has access.                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring MIB Views on page 1496</a></li> <li>• <a href="#">Configuring the Notify View on page 1515</a></li> </ul>                                                                                                 |

## oid

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>oid <i>oid</i> (include   exclude);</code>                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 notify-filter <i>profile-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Specify an object identifier (OID) used to represent a subtree of MIB objects. This OID is a prefix that the represented MIB objects have in common.                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>exclude</b> —Exclude the subtree of MIB objects represented by the specified OID.<br><br><b>include</b> —Include the subtree of MIB objects represented by the specified OID.<br><br><b>oid</b> —Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name. |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Trap Notification Filter on page 1522</a></li> </ul>                                                                                                                                                                                                                                                                                                                 |

## parameters

---

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>parameters {<br/>  message-processing-model (v1   v2c   v3);<br/>  security-level (none   authentication   privacy);<br/>  security-model (usm   v1   v2c);<br/>  security-name security-name;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-parameters <i>target-parameters-name</i> ]                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                  |
| <b>Description</b>              | Configure a set of target parameters for message processing and security.<br><br>The remaining statements are explained separately.                                                                             |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Defining and Configuring the Trap Target Parameters on page 1526</a></li></ul>                                                                              |

## port

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>port port-number;</pre>                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-address <i>target-address-name</i> ]                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure a UDP port number for an SNMP target.                                                                                                                                                |
| <b>Default</b>                  | If you omit this statement, the default port is 162.                                                                                                                                           |
| <b>Options</b>                  | <i>port-number</i> —Port number for the SNMP target.                                                                                                                                           |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Port on page 1524</a></li></ul>                                                                                            |



## privacy-3des

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>privacy-3des {   <b>privacy-password</b> <i>privacy-password</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <pre>[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i>]</pre>                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.</p>                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>privacy-password</b> <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> <li>• The password must be at least eight characters long.</li> <li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li> </ul> |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Encryption Type on page 1510</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                           |

## privacy-aes128

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>privacy-aes128 {<br/>    <b>privacy-password</b> <i>privacy-password</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm local-engine user <i>username</i> ],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> ]                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>privacy-password</b> <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"><li>• The password must be at least eight characters long.</li><li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li></ul> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the SNMPv3 Encryption Type on page 1510</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                          |

## privacy-des

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>privacy-des {<br/>    <b>privacy-password</b> <i>privacy-password</i>;<br/>}</code>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm local-engine user <i>username</i> ],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> ]                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>privacy-password</b> <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> <li>• The password must be at least eight characters long.</li> <li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li> </ul> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Encryption Type on page 1510</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                           |

## privacy-none

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>privacy-none;</code>                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm local-engine user <i>username</i> ],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> ]                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure that no encryption be used for the SNMPv3 user.                                                                                                                                      |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Encryption Type on page 1510</a></li> </ul>                                                                        |

## privacy-password

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>privacy-password <i>privacy-password</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm local-engine user <i>username</i> privacy-3des],<br>[edit snmp v3 usm local-engine user <i>username</i> privacy-aes128],<br>[edit snmp v3 usm local-engine user <i>username</i> privacy-des],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-3des],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-aes128],<br>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-des] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure a privacy password for the SNMPv3 user.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b><i>privacy-password</i></b>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"><li>• The password must be at least eight characters long.</li><li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li></ul>           |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the SNMPv3 Encryption Type on page 1510</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                   |

---

## read-view

---

|                                 |                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>read-view <i>view-name</i>;</code>                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [ <code>edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i>) security-model (any   usm   v1   v2c) security-level (authentication   none   privacy)</code> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                           |
| <b>Description</b>              | Associate the read-only view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).                                                                                                      |
| <b>Options</b>                  | <b><i>view-name</i></b> —The name of the view to which the SNMP user group has access.                                                                                                                                   |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Read View on page 1515</a></li><li>• <a href="#">Configuring MIB Views on page 1496</a></li></ul>                                                    |

## remote-engine

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> remote-engine <i>engine-id</i> {   user <i>username</i> {     authentication-md5 {       authentication-password <i>authentication-password</i>;     }     authentication-none;     authentication-sha {       authentication-password <i>authentication-password</i>;     }     privacy-aes128 {       privacy-password <i>privacy-password</i>;     }     privacy-des {       privacy-password <i>privacy-password</i>;     }     privacy-3des {       privacy-password <i>privacy-password</i>;     }     privacy-none {       privacy-password <i>privacy-password</i>;     }   } } </pre> |
| <b>Hierarchy Level</b>          | [edit snmp v3 usm]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Configure the remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b><i>engine-id</i></b>—Specify engine identifier in hexadecimal format. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring the Remote Engine and Remote User on page 1530</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

## routing-instance

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>routing-instance <i>routing-instance-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp v3 <a href="#">target-address</a> <i>target-address-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Specify a routing instance for an SNMPv3 trap target.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b><i>routing-instance-name</i></b>—Name of the routing instance.</p> <p>To configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash ( / ) to separate the two names (for example, <b>test-ls/test-ri</b>). To configure the default routing instance on a logical system, specify the logical system name followed by <b>default</b> (for example, <b>test-ls/default</b>).</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Trap Target Address on page 1522</a></li></ul>                                                                                                                                                                                                                                                                                                                                                  |

## security-level (Defining Access Privileges)

---

|                                 |                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>security-level (authentication   none   privacy) {<br/>    <b>notify-view</b> <i>view-name</i>;<br/>    <b>read-view</b> <i>view-name</i>;<br/>    <b>write-view</b> <i>view-name</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i> ) security-model (any   usm   v1   v2c)]                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.          |
| <b>Description</b>              | Define the security level used for access privileges.                                                                                                                                                   |
| <b>Default</b>                  | none                                                                                                                                                                                                    |
| <b>Options</b>                  | <b>authentication</b> —Provide authentication but no encryption.<br><br><b>none</b> —No authentication and no encryption.<br><br><b>privacy</b> —Provide authentication and encryption.                 |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Security Level on page 1514</a></li></ul>                                                                                           |



## security-level (Generating SNMP Notifications)

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | security-level (authentication   none   privacy);                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]                                                                                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the security level to use when generating SNMP notifications.                                                                                                                        |
| <b>Default</b>                  | none                                                                                                                                                                                           |
| <b>Options</b>                  | <b>authentication</b> —Provide authentication but no encryption.<br><br><b>none</b> —No authentication and no encryption.<br><br><b>privacy</b> —Provide authentication and encryption.        |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Security Level on page 1528</a></li></ul>                                                                                  |

## security-model (Access Privileges)

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>security-model (usm   v1   v2c);</code>                                                                                                                                                  |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i>)]</code>                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the security model for an SNMPv3 group. The security model is used to determine access privileges for the group.                                                                     |
| <b>Options</b>                  | <code>usm</code> —SNMPv3 security model.<br><br><code>v1</code> —SNMPv1 security model.<br><br><code>v2c</code> —SNMPv2c security model.                                                       |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Security Model on page 1514</a></li></ul>                                                                                  |

## security-model (Group)


|                                 |                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>security-model (usm   v1   v2c) {     security-name security-name {         group group-name;     } }</pre>              |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm <a href="#">security-to-group</a> ]                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.     |
| <b>Description</b>              | Define a security model for a group.                                                                                          |
| <b>Options</b>                  | <b>usm</b> —SNMPv3 security model.<br><br><b>v1</b> —SNMPv1 security model.<br><br><b>v2c</b> —SNMPv2c security model.        |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Security Model on page 1517</a></li> </ul>               |

## security-model (SNMP Notifications)

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | security-model (usm   v1   v2c);                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]                                                                                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the security model for an SNMPv3 group. The security model is used for SNMP notifications.                                                                                           |
| <b>Options</b>                  | <b>usm</b> —SNMPv3 security model.<br><br><b>v1</b> —SNMPv1 security model.<br><br><b>v2c</b> —SNMPv2c security model.                                                                         |
| <b>Required Privilege Level</b> | <b>snmp</b> —To view this statement in the configuration.<br><b>snmp-control</b> —To add this statement to the configuration.                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Security Model on page 1528</a></li> </ul>                                                                                |

## security-name (Community String)

---

|                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                          | <code>security-name <i>security-name</i>;</code>                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                 | <code>[edit snmp v3 <i>snmp-community</i> <i>community-index</i>]</code>                                                                                                                                                                                       |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                             | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                 |
| <b>Description</b>                                                                                                                                                                                                                                                                                                     | Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level. |
| <b>Options</b>                                                                                                                                                                                                                                                                                                         | <i>security-name</i> —Name that is used for messaging security and user access control.                                                                                                                                                                        |
| <div> <b>NOTE:</b> The security name must match the configured security name at the <code>[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]</code> hierarchy level when you configure traps or informs.</div> |                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                        | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                      |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Security Names on page 1538</a></li></ul>                                                                                                                                                  |


## security-name (Security Group)

---

|                                 |                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>security-name <i>security-name</i> {<br/>    group <i>group-name</i>;<br/>}</code>                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm security-to-group <b>security-model</b> (usm   v1   v2c)]                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                          |
| <b>Description</b>              | Associate a group or a community string with a configured security group.                                                                                                                                                                                                          |
| <b>Options</b>                  | <b>security-name</b> —Username configured at the [edit snmp v3 usm local-engine user <i>username</i> ] hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the [edit snmp v3 snmp-community <i>community-index</i> ] hierarchy level. |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Assigning Security Names to Groups on page 1518</a></li> </ul>                                                                                                                                                                |

## security-name (SNMP Notifications)

---

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>security-name <i>security-name</i>;</code>                                                                                                                                                                                              |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <code>[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]</code>                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Configure the security name used when generating SNMP notifications.                                                                                                                                                                          |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b><i>security-name</i></b> —If the SNMPv3 USM security model is used, identify the user when generating the SNMP notification. If the v1 or v2c security models are used, identify the SNMP community used when generating the notification. |
| <hr/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                               |
| <div> <b>NOTE:</b> The access privileges for the group associated with this security name must allow this notification to be sent.</div> <p>If you are using the v1 or v2 security models, the security name at the <code>[edit snmp v3 vacm security-to-group]</code> hierarchy level must match the security name at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level.</p> <hr/> |                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                     |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Security Name on page 1528</a></li></ul>                                                                                                                                  |

## security-to-group

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>security-to-group {   security-model (usm   v1   v2c) {     group group-name;     security-name security-name;   } }</pre>                                                                               |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm]                                                                                                                                                                                           |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> |
| <b>Description</b>              | <p>Configure the group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.</p> <p>The remaining statements are explained separately.</p>                      |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Assigning Security Model and Security Name to a Group on page 1517</a></li> </ul>                                                                        |

## snmp-community

|                                 |                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>snmp-community community-index {   community-name community-name;   security-name security-name;   tag tag-name; }</pre>                |
| <b>Hierarchy Level</b>          | [edit snmp v3]                                                                                                                               |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>         |
| <b>Description</b>              | Configure the SNMP community.                                                                                                                |
| <b>Options</b>                  | <p><b>community-index</b>—(Optional) String that identifies an SNMP community.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Community on page 1536</a></li> </ul>                            |

## tag

---

|                                 |                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>tag tag-name;</code>                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit snmp v3 <a href="#">notify name</a> ],<br>[edit snmp v3 <a href="#">snmp-community community-index</a> ]                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                          |
| <b>Description</b>              | Configure a set of targets to receive traps or informs (for IPv4 packets only).                                                                                                    |
| <b>Options</b>                  | <b>tag-name</b> —Identifies the address of managers that are allowed to use a community string.                                                                                    |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Tag on page 1538</a></li><li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1520</a></li></ul> |

## tag-list

---

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>tag-list tag-list;</code>                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit snmp v3 target-address <i>target-address-name</i> ]                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure an SNMP tag list used to select target addresses.                                                                                                                                    |
| <b>Options</b>                  | <b>tag-list</b> —Define sets of target addresses (tags). To specify more than one tag, specify the tag names as a space-separated list enclosed within double quotes.                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Trap Target Address on page 1524</a></li></ul>                                                                             |



## target-address

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>target-address <i>target-address-name</i> {   address <i>address</i>;   address-mask <i>address-mask</i>;   logical-system <i>logical-system</i>;   port <i>port-number</i>;   retry-count <i>number</i>;   routing-instance <i>instance</i>;   tag-list <i>tag-list</i>;   target-parameters <i>target-parameters-name</i>;   timeout <i>seconds</i>; }</pre> |
| <b>Hierarchy Level</b>          | [edit snmp v3]                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>                                                                                                                                                                                                                                |
| <b>Description</b>              | Configure the address of an SNMP management application and the parameters to be used in sending notifications.                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b><i>target-address-name</i></b>—String that identifies the target address.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Trap Target Address on page 1522</a></li> </ul>                                                                                                                                                                                                                                                |

## target-parameters

**Syntax** At the `[edit snmp v3]` hierarchy level:

```
target-parameters target-parameters-name {
 profile-name;
 parameters {
 message-processing-model (v1 | v2c | V3);
 security-level (authentication | none | privacy);
 security-model (usm | v1 | v2c);
 security-name security-name;
 }
}
```

At the `[edit snmp v3 target-address target-address-name]` hierarchy level:

```
target-parameters target-parameters-name;
```

**Hierarchy Level** `[edit snmp v3]`  
`[edit snmp v3 target-address target-address-name]`

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Configure the message processing and security parameters for sending notifications to a particular management target. The target parameters are configured at the `[edit snmp v3]` hierarchy level. The remaining statements at this level are explained separately.

Then apply the target parameters configured at the `[edit snmp v3 target-parameters target-parameters-name]` hierarchy level to the target address configuration at the `[edit snmp v3]` hierarchy level.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [Defining and Configuring the Trap Target Parameters on page 1526](#)
- [Applying Target Parameters on page 1525](#)

## type

---

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>type (inform   trap);</code>                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 notify <i>name</i>]</code>                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br><b>inform</b> option added in Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Configure the type of SNMP notification.                                                                                                                                                                                                              |
| <b>Options</b>                  | <b>inform</b> —Defines the type of notification as an inform. SNMP informs are confirmed notifications.<br><br><b>trap</b> —Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.                                     |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring SNMP Informs on page 1529</a></li> <li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1520</a></li> </ul>                                                            |

## user

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>user <i>username</i>;</code>                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit snmp v3 usm local-engine],</code><br><code>[edit snmp v3 usm remote-engine <i>engine-id</i>]</code>                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Specify a user associated with an SNMPv3 group on a local or remote SNMP engine.                                                                                                                                                                                           |
| <b>Options</b>                  | <b><i>username</i></b> —SNMPv3 user-based security model (USM) username.                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <code>snmp</code> —To view this statement in the configuration.<br><code>snmp-control</code> —To add this statement to the configuration.                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Creating SNMPv3 Users on page 1507</a></li> </ul>                                                                                                                                                                     |

## usm

```

Syntax usm {
 local-engine {
 user username {
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-none;
 authentication-sha {
 authentication-password authentication-password;
 }
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none {
 privacy-password privacy-password;
 }
 }
 }
 remote-engine engine-id {
 user username {
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-none;
 authentication-sha {
 authentication-password authentication-password;
 }
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none {
 privacy-password privacy-password;
 }
 }
 }
 }
}

```

Hierarchy Level [edit snmp v3]

Release Information Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

|                                 |                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>              | Configure user-based security model (USM) information.<br><br>The remaining statements are explained separately.                                                                          |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Creating SNMPv3 Users on page 1507</a></li><li>• <a href="#">Configuring the Remote Engine and Remote User on page 1530</a></li></ul> |

## v3

```

Syntax v3 {
 notify name {
 tag tag-name;
 type trap;
 }
 notify-filter profile-name {
 oid object-identifier (include | exclude);
 }
 snmp-community community-index {
 community-name community-name;
 security-name security-name;
 tag tag-name;
 }
 target-address target-address-name {
 address address;
 address-mask address-mask;
 logical-system logical-system;
 port port-number;
 retry-count number;
 routing-instance instance;
 tag-list tag-list;
 target-parameters target-parameters-name;
 timeout seconds;
 }
 target-parameters target-parameters-name {
 notify-filter profile-name;
 parameters {
 message-processing-model (v1 | v2c | V3);
 security-level (authentication | none | privacy);
 security-model (usm | v1 | v2c);
 security-name security-name;
 }
 }
 usm {
 local-engine {
 user username {
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-sha {
 authentication-password authentication-password;
 }
 authentication-none;
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 }
 }
 }
}

```

```

 privacy-none;
 }
}
remote-engine engine-id {
 user username {
 authentication-md5 {
 authentication-password authentication-password;
 }
 authentication-sha {
 authentication-password authentication-password;
 }
 authentication-none;
 privacy-aes128 {
 privacy-password privacy-password;
 }
 privacy-des {
 privacy-password privacy-password;
 }
 privacy-3des {
 privacy-password privacy-password;
 }
 privacy-none {
 privacy-password privacy-password;
 }
 }
}
}
vacm {
 access {
 group group-name {
 (default-context-prefix | context-prefix context-prefix) {
 security-model (any | usm | v1 | v2c) {
 security-level (authentication | none | privacy) {
 notify-view view-name;
 read-view view-name;
 write-view view-name;
 }
 }
 }
 }
 }
}
security-to-group {
 security-model (usm | v1 | v2c) {
 security-name security-name {
 group group-name;
 }
 }
}
}
}

```

Hierarchy Level [edit snmp]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

|                                 |                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>              | Configure SNMPv3.<br><br>The remaining statements are explained separately.                                                              |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1502</a></li></ul> |

---

## vacm

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>vacm {<br/>  access {<br/>    group group-name {<br/>      (default-context-prefix   context-prefix <i>context-prefix</i>){<br/>        security-model (any   usm   v1   v2c) {<br/>          security-level (authentication   none   privacy) {<br/>            notify-view view-name;<br/>            read-view view-name;<br/>            write-view view-name;<br/>          }<br/>        }<br/>      }<br/>    }<br/>  }<br/>  security-to-group {<br/>    security-model (usm   v1   v2c);<br/>    security-name security-name {<br/>      group group-name;<br/>    }<br/>  }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit snmp <b>v3</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Configure view-based access control model (VACM) information.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Defining Access Privileges for an SNMP Group on page 1512</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



---

## write-view

---

|                                 |                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>write-view view-name;</code>                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i> ) security-model (any   usm   v1   v2c) security-level (authentication   none   privacy)]                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>              | Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).                                                                                                                                                                   |
| <b>Options</b>                  | <b><i>view-name</i></b> —Name of the view for which the SNMP user group has write permission.                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring MIB Views on page 1496</a></li><li>• <a href="#">Configuring the Write View on page 1516</a></li></ul>                                                                                                            |



## CHAPTER 101

# Operational Commands

- clear chassis cluster ip-monitoring failure-count
- clear chassis cluster ip-monitoring failure-count ip-address
- clear ilmi statistics
- clear snmp history
- clear snmp statistics
- request pppoe connect
- request pppoe disconnect
- request services ip-monitoring preempt-restore policy
- request snmp spoof-trap
- show chassis alarms
- show chassis cluster ip-monitoring status redundancy-group
- show interfaces (SRX Series)
- show interfaces snmp-index
- show interfaces summary
- show ilmi statistics
- show security alarms
- show security datapath-debug capture
- show security datapath-debug counter
- show security monitoring
- show security monitoring fpc fpc-number
- show security monitoring performance session
- show security monitoring performance spu
- show services ip-monitoring status
- show snmp health-monitor
- show snmp inform-statistics
- show snmp mib
- show snmp rmon
- show snmp statistics

- [show snmp stats-response-statistics](#)
- [show snmp v3](#)
- [show system alarms](#)
- [show system resource-monitor fpc](#)

## clear chassis cluster ip-monitoring failure-count

---

|                                 |                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear chassis cluster ip-monitoring failure-count                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1.                                                                                                                                                                            |
| <b>Description</b>              | Clear the failure count for all IP addresses.                                                                                                                                                                           |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">clear chassis cluster ip-monitoring failure-count</a></li><li>• <a href="#">clear chassis cluster ip-monitoring failure-count ip-address on page 2118</a></li></ul> |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                   |

### Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count
node0:

Cleared failure count for all IPs

node1:

Cleared failure count for all IPs
```

## clear chassis cluster ip-monitoring failure-count ip-address

---

|                            |                                                                      |
|----------------------------|----------------------------------------------------------------------|
| <b>Syntax</b>              | clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1 |
| <b>Release Information</b> | Command introduced in Junos OS Release 10.1.                         |
| <b>Description</b>         | Clear the failure count for a specified IP address.                  |



**NOTE:** Entering an IP address at the end of this command is optional. If you do not specify an IP address, the failure count for all monitored IP addresses is cleared.

|                                 |                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>clear chassis cluster failover-count</i></li><li>• <a href="#">clear chassis cluster ip-monitoring failure-count on page 2117</a></li></ul> |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                  |

### Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1
node0:

Cleared failure count for IP: 1.1.1.1

node1:

Cleared failure count for IP: 1.1.1.1
```

## clear ilmi statistics

---

|                                 |                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear ilmi statistics                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                     |
| <b>Description</b>              | Set Integrated Local Management Interface (ILMI) statistics to zero.                                |
| <b>Options</b>                  | This command has no options.                                                                        |
| <b>Required Privilege Level</b> | clear                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show ilmi statistics on page 2171</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear ilmi statistics on page 2119</a>                                                  |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.               |

### Sample Output

#### clear ilmi statistics

```
user@host> clear ilmi statistics
```

## clear snmp history

---

|                                 |                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear snmp history ( <i>index</i>   all)                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Delete the history record of Simple Network Management Protocol (SNMP) samples of Ethernet statistics collected.                                                                         |
| <b>Options</b>                  | <b>all</b> —Clear all the entries in the history index.<br><br><b>index</b> —Clear the contents of the specified entry in the history index.                                             |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">clear snmp statistics on page 2121</a></li></ul>                                                                                     |



## clear snmp statistics

|                                 |                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear snmp statistics                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series. |
| <b>Description</b>              | Clear Simple Network Management Protocol (SNMP) statistics.                                                                                                                              |
| <b>Options</b>                  | This command has no options.                                                                                                                                                             |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show snmp statistics on page 2207</a></li> </ul>                                                                                    |
| <b>List of Sample Output</b>    | <a href="#">clear snmp statistics on page 2121</a>                                                                                                                                       |
| <b>Output Fields</b>            | See <a href="#">show snmp statistics</a> for an explanation of output fields.                                                                                                            |

## Sample Output

### clear snmp statistics

In the following example, SNMP statistics are displayed before and after the **clear snmp statistics** command is issued:

```

user@host> show snmp statistics
SNMP statistics:
 Input:
 Packets: 8, Bad versions: 0, Bad community names: 0,
 Bad community uses: 0, ASN parse errors: 0,
 Too bigs: 0, No such names: 0, Bad values: 0,
 Read onlys: 0, General errors: 0,
 Total request varbinds: 8, Total set varbinds: 0,
 Get requests: 0, Get nexts: 8, Set requests: 0,
 Get responses: 0, Traps: 0,
 Silent drops: 0, Proxy drops 0
 Output:
 Packets: 2298, Too bigs: 0, No such names: 0,
 Bad values: 0, General errors: 0,
 Get requests: 0, Get nexts: 0, Set requests: 0,
 Get responses: 8, Traps: 2290

user@host> clear snmp statistics

user@host> show snmp statistics
SNMP statistics:
 Input:
 Packets: 0, Bad versions: 0, Bad community names: 0,
 Bad community uses: 0, ASN parse errors: 0,
 Too bigs: 0, No such names: 0, Bad values: 0,
 Read onlys: 0, General errors: 0,

```

```
Total request varbinds: 0, Total set varbinds: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0,
Silent drops: 0, Proxy drops 0
Output:
Packets: 0, Too bigs: 0, No such names: 0,
Bad values: 0, General errors: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0
```

## request pppoe connect

---

|                                 |                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request pppoe connect                                                                            |
| <b>Release Information</b>      | Statement supported on SRX300, SRX320, and SRX340 is introduced in Junos OS Release 15.1X49-D60. |
| <b>Description</b>              | Connect all sessions that are down.                                                              |
| <b>Options</b>                  | <b>pppoe interface name</b> — (Optional) Connect to a specified session.                         |
| <b>Required Privilege Level</b> | maintenance                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">request pppoe connect on page 2123</a>                                               |
| <b>Output Fields</b>            | When you enter this command, this command returns no output.                                     |

### Sample Output

request pppoe connect

```
user@host> request pppoe connect
```

## request pppoe disconnect

---


|                                 |                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request pppoe disconnect                                                                                                                                                                             |
| <b>Release Information</b>      | Statement supported on SRX300, SRX320, and SRX340 is introduced in Junos OS Release 15.1X49-D60.                                                                                                     |
| <b>Description</b>              | Disconnect all active sessions.                                                                                                                                                                      |
| <b>Options</b>                  | <b>session id</b> — (Optional) Disconnect the session for which the session ID is specified.<br><b>pppoe interface name</b> — (Optional) Disconnect the session for a specific pppoe interface name. |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">request pppoe disconnect on page 2124</a>                                                                                                                                                |
| <b>Output Fields</b>            | When you enter this command, this command returns no output.                                                                                                                                         |

### Sample Output

#### request pppoe disconnect

```
user@host> request pppoe disconnect
```

## request services ip-monitoring preempt-restore policy

|                                 |                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>request services ip-monitoring preempt-restore policy</b><br><i>&lt;policy-name&gt;</i>                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.4.                                                                                                                                                                                                                                                       |
| <b>Description</b>              | If the no-preempt option is specified, the policy will not perform preemptive failback when it is in a failover state, and when the RPM probe test recovers from failure. To manually revert to the failback state, run the <b>request services ip-monitoring preempt-restore policy</b> command.  |
|                                 | <div>  <p><b>NOTE:</b> The <b>request services ip-monitoring preempt-restore policy</b> command takes effect only when the RPM probe is in the pass state, and when the policy is in a failover state.</p> </div> |
| <b>Options</b>                  | <b>policy name</b> —Name of the policy.                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show services rpm probe-results (View)</a></li> <li>• <a href="#">show services ip-monitoring status on page 2187</a></li> </ul>                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">run request services ip-monitoring preempt-restore policy &lt;policy name&gt; on page 2125</a>                                                                                                                                                                                         |
| <b>Output Fields</b>            | When you run this command, the policy is restored to the failback state.                                                                                                                                                                                                                           |

### Sample Output

run request services ip-monitoring preempt-restore policy <policy name>

```
user@host> run request services ip-monitoring preempt-restore policy policy1
Restore request succeeded: Policy policy1
```

## request snmp spoof-trap

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>request snmp spoof-trap</b><br><b>&lt;trap&gt; variable-bindings &lt;object&gt; &lt;instance&gt; &lt;value&gt;</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.2.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>&lt;trap&gt;</b>—Name of the trap to spoof.</p> <p><b>variable-bindings &lt;object&gt; &lt;instance&gt; &lt;value&gt;</b>—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, <b>ifIndex[14] = 14</b>). Enclose the list of variable bindings in quotation marks ( " ") and use a comma to separate each object name, instance, and value definition (for example, <b>variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"</b>). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.</p> <p><b>&lt;dummy name&gt;</b>—A dummy trap name to display the list of available traps.</p> <p><b>Question mark (?)</b>—Question mark? to display possible completions.</p> |
| <b>Required Privilege Level</b> | request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">request snmp spoof-trap (with Variable Bindings) on page 2126</a><br><a href="#">request snmp spoof-trap (Illegal Trap Name) on page 2126</a><br><a href="#">request snmp spoof-trap (Question Mark ?) on page 2130</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Sample Output

### request snmp spoof-trap (with Variable Bindings)

```
user@host> request snmp spoof-trap linkUp variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"
Spoof trap request result: trap sent successfully
```

### request snmp spoof-trap (Illegal Trap Name)

```
user@host> request snmp spoof-trap xx
Spoof trap request result: trap not found
```

```
Allowed Traps:
ads1AtucInitFailureTrap
ads1AtucPerfESsThreshTrap
ads1AtucPerfLofsThreshTrap
ads1AtucPerfLolsThreshTrap
ads1AtucPerfLossThreshTrap
ads1AtucPerfLprsThreshTrap
ads1AtucRateChangeTrap
```

ads1AturPerfESsThreshTrap  
ads1AturPerfLofsThreshTrap  
ads1AturPerfLossThreshTrap  
ads1AturPerfLprsThreshTrap  
ads1AturRateChangeTrap  
apsEventChannelMismatch  
apsEventFEPLF  
apsEventModeMismatch  
apsEventPSBF  
apsEventSwitchover  
authenticationFailure  
bfdSessDown  
bfdSessUp  
bgpBackwardTransition  
bgpEstablished  
coldStart  
dlswTrapCircuitDown  
dlswTrapCircuitUp  
dlswTrapTConnDown  
dlswTrapTConnPartnerReject  
dlswTrapTConnProtViolation  
dlswTrapTConnUp  
dsx1LineStatusChange  
dsx3LineStatusChange  
entConfigChange  
fallingAlarm  
frDLCIStatusChange  
ggsnTrapChanged  
ggsnTrapCleared  
ggsnTrapNew  
gmplsTunnelDown  
ifMauJabberTrap  
ipv6IfStateChange  
isisAreaMismatch  
isisAttemptToExceedMaxSequence  
isisAuthenticationFailure  
isisAuthenticationTypeFailure  
isisCorruptedLSPDetected  
isisDatabaseOverload  
isisIDLenMismatch  
isisLSPTooLargeToPropagate  
isisManualAddressDrops  
isisMaxAreaAddressesMismatch  
isisOriginatingLSPBufferSizeMismatch  
isisOwnLSPPurge  
isisProtocolsSupportedMismatch  
isisRejectedAdjacency  
isisSequenceNumberSkip  
isisVersionSkew  
jnxAccessAuthServerDisabled  
jnxAccessAuthServerEnabled  
jnxAccessAuthServiceDown  
jnxAccessAuthServiceUp  
jnxBfdSessDetectionTimeHigh  
jnxBfdSessTxIntervalHigh  
jnxBgpM2BackwardTransition  
jnxBgpM2Established  
jnxCmCfgChange  
jnxCmRescueChange  
jnxCollFlowOverload  
jnxCollFlowOverloadCleared

jnxCollFtpSwitchover  
jnxCollMemoryAvailable  
jnxCollMemoryUnavailable  
jnxCollUnavailableDest  
jnxCollUnavailableDestCleared  
jnxCollUnsuccessfulTransfer  
jnxDfcHardMemThresholdExceeded  
jnxDfcHardMemUnderThreshold  
jnxDfcHardPpsThresholdExceeded  
jnxDfcHardPpsUnderThreshold  
jnxDfcSoftMemThresholdExceeded  
jnxDfcSoftMemUnderThreshold  
jnxDfcSoftPpsThresholdExceeded  
jnxDfcSoftPpsUnderThreshold  
jnxEventTrap  
jnxExampleStartup  
jnxFEBSwitchover  
jnxFanFailure  
jnxFanOK  
jnxFruCheck  
jnxFruFailed  
jnxFruInsertion  
jnxFruOK  
jnxFruOffline  
jnxFruOnline  
jnxFruPowerOff  
jnxFruPowerOn  
jnxFruRemoval  
jnxHardDiskFailed  
jnxHardDiskMissing  
jnxJsAvPatternUpdateTrap  
jnxJsChassisClusterSwitchover  
jnxJsFwAuthCapacityExceeded  
jnxJsFwAuthFailure  
jnxJsFwAuthServiceDown  
jnxJsFwAuthServiceUp  
jnxJsNatAddrPoolThresholdStatus  
jnxJsScreenAttack  
jnxJsScreenCfgChange  
jnxLdpLspDown  
jnxLdpLspUp  
jnxLdpSesDown  
jnxLdpSesUp  
jnxMIMstCistPortLoopProtectStateChangeTrap  
jnxMIMstCistPortRootProtectStateChangeTrap  
jnxMIMstErrTrap  
jnxMIMstGenTrap  
jnxMIMstInvalidBpduRxdTrap  
jnxMIMstMstiPortLoopProtectStateChangeTrap  
jnxMIMstMstiPortRootProtectStateChangeTrap  
jnxMIMstNewRootTrap  
jnxMIMstProtocolMigrationTrap  
jnxMIMstRegionConfigChangeTrap  
jnxMIMstTopologyChgTrap  
jnxMacChangedNotification  
jnxMplsLdpInitSesThresholdExceeded  
jnxMplsLdpPathVectorLimitMismatch  
jnxMplsLdpSessionDown  
jnxMplsLdpSessionUp  
jnxOspfV3IfConfigError  
jnxOspfV3IfRxBadPacket



jnxOspfV3IfStateChange  
jnxOspfV3LsdbApproachingOverflow  
jnxOspfV3LsdbOverflow  
jnxOspfV3NbrRestartHelperStatusChange  
jnxOspfV3NbrStateChange  
jnxOspfV3NssaTranslatorStatusChange  
jnxOspfV3RestartStatusChange  
jnxOspfV3VirtIfConfigError  
jnxOspfV3VirtIfRxBadPacket  
jnxOspfV3VirtIfStateChange  
jnxOspfV3VirtNbrRestartHelperStatusChange  
jnxOspfV3VirtNbrStateChange  
jnxOtnAlarmCleared  
jnxOtnAlarmSet  
jnxOverTemperature  
jnxPmonOverloadCleared  
jnxPmonOverloadSet  
jnxPingEgressJitterThresholdExceeded  
jnxPingEgressStdDevThresholdExceeded  
jnxPingEgressThresholdExceeded  
jnxPingIngressJitterThresholdExceeded  
jnxPingIngressStdDevThresholdExceeded  
jnxPingIngressThresholdExceeded  
jnxPingRttJitterThresholdExceeded  
jnxPingRttStdDevThresholdExceeded  
jnxPingRttThresholdExceeded  
jnxPortBpduErrorStatusChangeTrap  
jnxPortLoopProtectStateChangeTrap  
jnxPortRootProtectStateChangeTrap  
jnxPowerSupplyFailure  
jnxPowerSupplyOK  
jnxRedundancySwitchover  
jnxRmonAlarmGetFailure  
jnxRmonGetOk  
jnxSecAccessIfMacLimitExceeded  
jnxSecAccessSdsRateLimitCrossed  
jnxSonetAlarmCleared  
jnxSonetAlarmSet  
jnxSpSvcSetCpuExceeded  
jnxSpSvcSetCpuOk  
jnxSpSvcSetZoneEntered  
jnxSpSvcSetZoneExited  
jnxStormEventNotification  
jnxSyslogTrap  
jnxTemperatureOK  
jnxVccpPortDown  
jnxVccpPortUp  
jnxVpnIfDown  
jnxVpnIfUp  
jnxVpnPwDown  
jnxVpnPwUp  
jnx12aldGlobalMacLimit  
jnx12aldInterfaceMacLimit  
jnx12aldRoutingInstMacLimit  
linkDown  
linkUp  
lldpRemTablesChange  
mfrMibTrapBundleLinkMismatch  
mplsLspChange  
mplsLspDown  
mplsLspInfoChange

mplsLspInfoDown  
mplsLspInfoPathDown  
mplsLspInfoPathUp  
mplsLspInfoUp  
mplsLspPathDown  
mplsLspPathUp  
mplsLspUp  
mplsNumVrfRouteMaxThreshExceeded  
mplsNumVrfRouteMidThreshExceeded  
mplsNumVrfSecIllglLb1ThrshExcd  
mplsTunnelDown  
mplsTunnelReoptimized  
mplsTunnelRerouted  
mplsTunnelUp  
mplsVrfIfDown  
mplsVrfIfUp  
mplsXCDown  
mplsXCUp  
msdpBackwardTransition  
msdpEstablished  
newRoot  
ospfIfAuthFailure  
ospfIfConfigError  
ospfIfRxBadPacket  
ospfIfStateChange  
ospfLsdbApproachingOverflow  
ospfLsdbOverflow  
ospfMaxAgeLsa  
ospfNbrStateChange  
ospfOriginateLsa  
ospfTxRetransmit  
ospfVirtIfAuthFailure  
ospfVirtIfConfigError  
ospfVirtIfRxBadPacket  
ospfVirtIfStateChange  
ospfVirtIfTxRetransmit  
ospfVirtNbrStateChange  
pethMainPowerUsageOffNotification  
pethMainPowerUsageOnNotification  
pethPsePortOnOffNotification  
pingProbeFailed  
pingTestCompleted  
pingTestFailed  
ptopoConfigChange  
risingAlarm  
rpMauJabberTrap  
sd1cLSStatusChange  
sd1cPortStatusChange  
topologyChange  
traceRoutePathChange  
traceRouteTestCompleted  
traceRouteTestFailed  
vrrpTrapAuthFailure  
vrrpTrapNewMaster  
warmStart

#### request snmp spoof-trap (Question Mark ?)

```
user@host> request snmp spoof-trap ?
```

Possible completions:

```
<trap> The name of the trap to spoof
```

```
ads1AtucInitFailureTrap
ads1AtucPerfESsThreshTrap
ads1AtucPerfLofsThreshTrap
ads1AtucPerfLoIsThreshTrap
ads1AtucPerfLossThreshTrap
ads1AtucPerfLprsThreshTrap
ads1AtucRateChangeTrap
ads1AturPerfESsThreshTrap
ads1AturPerfLofsThreshTrap
ads1AturPerfLossThreshTrap
ads1AturPerfLprsThreshTrap
ads1AturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlsWTrapCircuitDown
dlsWTrapCircuitUp
---(more 10%)---
```

## show chassis alarms

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show chassis alarms                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for SRX Series devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Display information about the conditions that have been configured to trigger alarms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Additional Information</b>   | <p>You cannot clear the alarms for chassis components. Instead, you must remedy the cause of the alarm. When a chassis alarm is lit, it indicates that you are running the device in a manner that we do not recommend.</p> <p>On routers, you can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button, located on the craft interface. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after you silence an external device reactivate the external device.</p> <p>In Junos OS Release 11.1 and later, alarms for fans also show the slot number of the fans in the CLI output.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show system alarms on page 2220</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show chassis alarms on page 2132</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 235</a> lists the output fields for the <b>show chassis alarms</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 235: show chassis alarms Output Fields**

| Field Name         | Field Description                              |
|--------------------|------------------------------------------------|
| <b>Alarm time</b>  | Date and time the alarm was first recorded.    |
| <b>Class</b>       | Severity class for this alarm: Minor or Major. |
| <b>Description</b> | Information about the alarm.                   |

## Sample Output

### show chassis alarms

```
user@host> show chassis alarms
```

4 alarms currently active

| Alarm time              | Class | Description                                      |
|-------------------------|-------|--------------------------------------------------|
| 2012-05-29 16:47:18 UTC | Major | /var partition usage crossed critical threshold  |
| 2012-05-29 16:47:18 UTC | Minor | /var partition usage crossed high threshold      |
| 2012-05-29 16:47:18 UTC | Major | /root partition usage crossed critical threshold |
| 2012-05-29 16:47:18 UTC | Minor | /root partition usage crossed high threshold     |

## show chassis cluster ip-monitoring status redundancy-group

|                                 |                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show chassis cluster ip-monitoring status</b><br><b>&lt;redundancy-group group-number&gt;</b>                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.6. Support for global threshold, current threshold, and weight of each monitored IP address added in Junos OS Release 12.1X47-D10.                                                                                                           |
| <b>Description</b>              | Display the status of all monitored IP addresses for a redundancy group.                                                                                                                                                                                                              |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>none</b>— Display the status of monitored IP addresses for all redundancy groups on the node.</li> <li><b>redundancy-group group-number</b> — Display the status of monitored IP addresses under the specified redundancy group.</li> </ul> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear chassis cluster failover-count</a></li> </ul>                                                                                                                                                                                |
| <b>List of Sample Output</b>    | <a href="#">show chassis cluster ip-monitoring status on page 2135</a><br><a href="#">show chassis cluster ip-monitoring status redundancy-group on page 2136</a>                                                                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 236</a> lists the output fields for the <b>show chassis cluster ip-monitoring status</b> command.                                                                                                                                                                   |

**Table 236: show chassis cluster ip-monitoring status Output Fields**

| Field Name               | Field Description                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Redundancy-group</b>  | ID number (0 - 255) of a redundancy group in the cluster.                                                                                                                                                                                          |
| <b>Global threshold</b>  | Failover value for all IP addresses monitored by the redundancy group.                                                                                                                                                                             |
| <b>Current threshold</b> | Value equal to the global threshold minus the total weight of the unreachable IP address.                                                                                                                                                          |
| <b>IP Address</b>        | Monitored IP address in the redundancy group.                                                                                                                                                                                                      |
| <b>Status</b>            | <p>Current reachability state of the monitored IP address.</p> <p>Values for this field are: <b>reachable</b>, <b>unreachable</b>, and <b>unknown</b>. The status is “unknown” if Packet Forwarding Engines (PFEs) are not yet up and running.</p> |
| <b>Failure count</b>     | Number of attempts to reach an IP address.                                                                                                                                                                                                         |
| <b>Reason</b>            | Explanation for the reported status. See <a href="#">Table 237</a> .                                                                                                                                                                               |
| <b>Weight</b>            | Combined weight (0 - 255) assigned to all monitored IP addresses. A higher weight value indicates greater importance.                                                                                                                              |

Expanded reason output fields for unreachable IP addresses added in Junos OS Release 10.1. You might see any of the following reasons displayed.

**Table 237: show chassis cluster ip-monitoring status redundancy group Reason Fields**

| Reason                         | Reason Description                                                                                                                                               |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No route to host               | The router could not resolve the ARP, which is needed to send the ICMP packet to the host with the monitored IP address.                                         |
| No auxiliary IP found          | The redundant Ethernet interface does not have an auxiliary IP address configured.                                                                               |
| Reth child not up              | A child interface of a redundant Ethernet interface is down.                                                                                                     |
| redundancy-group state unknown | Unable to obtain the state (primary, secondary, secondary-hold, disable) of a redundancy-group.                                                                  |
| No reth child MAC address      | Could not extract the MAC address of the redundant Ethernet child interface.                                                                                     |
| Secondary link not monitored   | The secondary link might be down (the secondary child interface of a redundant Ethernet interface is either down or non-functional).                             |
| Unknown                        | The IP address has just been configured and the router still does not know the status of this IP.<br><br>or<br><br>Do not know the exact reason for the failure. |

## Sample Output

### show chassis cluster ip-monitoring status

```
user@host> show chassis cluster ip-monitoring status
node0:
```

```

Redundancy group: 1
Global threshold: 200
Current threshold: -120
```

| IP address  | Status    | Failure count | Reason | Weight |
|-------------|-----------|---------------|--------|--------|
| 10.254.5.44 | reachable | 0             | n/a    | 220    |
| 2.2.2.1     | reachable | 0             | n/a    | 100    |

```
node1:
```

```

Redundancy group: 1
Global threshold: 200
Current threshold: -120
```

| IP address  | Status    | Failure count | Reason | Weight |
|-------------|-----------|---------------|--------|--------|
| 10.254.5.44 | reachable | 0             | n/a    | 220    |
| 2.2.2.1     | reachable | 0             | n/a    | 100    |

## Sample Output

### show chassis cluster ip-monitoring status redundancy-group

```
user@host> show chassis cluster ip-monitoring status redundancy-group 1
node0:
```

-----

Redundancy group: 1

| IP address  | Status    | Failure count | Reason |
|-------------|-----------|---------------|--------|
| 10.254.5.44 | reachable | 0             | n/a    |
| 2.2.2.1     | reachable | 0             | n/a    |
| 1.1.1.5     | reachable | 0             | n/a    |
| 1.1.1.4     | reachable | 0             | n/a    |
| 1.1.1.1     | reachable | 0             | n/a    |

node1:

-----

Redundancy group: 1

| IP address  | Status    | Failure count | Reason |
|-------------|-----------|---------------|--------|
| 10.254.5.44 | reachable | 0             | n/a    |
| 2.2.2.1     | reachable | 0             | n/a    |
| 1.1.1.5     | reachable | 0             | n/a    |
| 1.1.1.4     | reachable | 0             | n/a    |
| 1.1.1.1     | reachable | 0             | n/a    |



## show interfaces (SRX Series)

**Syntax** show interfaces {  
 <brief | detail | extensive | terse>  
 controller *interface-name*  
 descriptions *interface-name*  
 destination-class (all | *destination-class-name logical-interface-name*)  
 diagnostics optics *interface-name*  
 far-end-interval *interface-fpc/pic/port*  
 filters *interface-name*  
 flow-statistics *interface-name*  
 interval *interface-name*  
 load-balancing (detail | *interface-name*)  
 mac-database mac-address *mac-address*  
 mc-ae id *identifier* unit *number* revertive-info  
 media *interface-name*  
 policers *interface-name*  
 queue both-ingress-egress egress forwarding-class *forwarding-class* ingress l2-statistics  
 redundancy (detail | *interface-name*)  
 routing brief detail summary *interface-name*  
 routing-instance (all | *instance-name*)  
 snmp-index *snmp-index*  
 source-class (all | *destination-class-name logical-interface-name*)  
 statistics *interface-name*  
 switch-port *switch-port number*  
 transport pm (all | optics | otn) (all | current | currentday | interval | previousday) (all |  
   *interface-name*)  
 zone *interface-name*  
 }

**Release Information** Command modified in Junos OS Release 9.5.

**Description** Display status information and statistics about interfaces on SRX Series appliance running Junos OS.

On SRX Series appliance, on configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

- Options**
- **interface-name**—(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number.
    - **at-*pim*/0/*port***—ATM-over-ADSL or ATM-over-SHDSL interface.
    - **ce1-*pim*/0/ *port***—Channelized E1 interface.
    - **cl-0/0/8**—3G wireless modem interface for SRX320 devices.
    - **ct1-*pim*/0/*port***—Channelized T1 interface.
    - **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
    - **e1-*pim*/0/*port***—E1 interface.
    - **e3-*pim*/0/*port***—E3 interface.

- **fe-pim/0/port**—Fast Ethernet interface.
- **ge-pim/0/port**—Gigabit Ethernet interface.
- **se-pim/0/port**—Serial interface.
- **t1-pim/0/port**—T1 (also called DS1) interface.
- **t3-pim/0/port**—T3 (also called DS3) interface.
- **wx-slot/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).
  
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output.
- **controller**—(Optional) Show controller information.
- **descriptions**—(Optional) Display interface description strings.
- **destination-class**—(Optional) Show statistics for destination class.
- **diagnostics**—(Optional) Show interface diagnostics information.
- **far-end-interval**—(Optional) Show far end interval statistics.
- **filters**—(Optional) Show interface filters information.
- **flow-statistics**—(Optional) Show security flow counters and errors.
- **interval**—(Optional) Show interval statistics.
- **load-balancing**—(Optional) Show load-balancing status.
- **mac-database**—(Optional) Show media access control database information.
- **mc-ae**—(Optional) Show MC-AE configured interface information.
- **media**—(Optional) Display media information.
- **policers**—(Optional) Show interface policers information.
- **queue**—(Optional) Show queue statistics for this interface.
- **redundancy**—(Optional) Show redundancy status.
- **routing**—(Optional) Show routing status.
- **routing-instance**—(Optional) Name of routing instance.
- **snmp-index**—(Optional) SNMP index of interface.
- **source-class**—(Optional) Show statistics for source class.
- **statistics**—(Optional) Display statistics and detailed output.
- **switch-port**—(Optional) Front end port number (0..15).
- **transport**—(Optional) Show interface transport information.
- **zone**—(Optional) Interface's zone.

**Required Privilege Level**    view

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Related Documentation</b></p> | <ul style="list-style-type: none"> <li>• <i>Understanding Interfaces</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>List of Sample Output</b></p> | <p> <a href="#">show interfaces Gigabit Ethernet on page 2146</a><br/> <a href="#">show interfaces brief (Gigabit Ethernet) on page 2147</a><br/> <a href="#">show interfaces detail (Gigabit Ethernet) on page 2147</a><br/> <a href="#">show interfaces extensive (Gigabit Ethernet) on page 2149</a><br/> <a href="#">show interfaces terse on page 2152</a><br/> <a href="#">show interfaces controller (Channelized E1 IQ with Logical E1) on page 2152</a><br/> <a href="#">show interfaces controller (Channelized E1 IQ with Logical DS0) on page 2152</a><br/> <a href="#">show interfaces descriptions on page 2153</a><br/> <a href="#">show interfaces destination-class all on page 2153</a><br/> <a href="#">show interfaces diagnostics optics on page 2153</a><br/> <a href="#">show interfaces far-end-interval coc12-5/2/0 on page 2154</a><br/> <a href="#">show interfaces far-end-interval coc1-5/2/1:1 on page 2154</a><br/> <a href="#">show interfaces filters on page 2155</a><br/> <a href="#">show interfaces flow-statistics (Gigabit Ethernet) on page 2155</a><br/> <a href="#">show interfaces interval (Channelized OC12) on page 2156</a><br/> <a href="#">show interfaces interval (E3) on page 2156</a><br/> <a href="#">show interfaces interval (SONET/SDH) on page 2157</a><br/> <a href="#">show interfaces load-balancing on page 2157</a><br/> <a href="#">show interfaces load-balancing detail on page 2157</a><br/> <a href="#">show interfaces mac-database (All MAC Addresses on a Port) on page 2158</a><br/> <a href="#">show interfaces mac-database (All MAC Addresses on a Service) on page 2158</a><br/> <a href="#">show interfaces mac-database mac-address on page 2159</a><br/> <a href="#">show interfaces mc-ae on page 2159</a><br/> <a href="#">show interfaces media (SONET/SDH) on page 2159</a><br/> <a href="#">show interfaces policers on page 2160</a><br/> <a href="#">show interfaces policers interface-name on page 2160</a><br/> <a href="#">show interfaces queue on page 2160</a><br/> <a href="#">show interfaces redundancy on page 2161</a><br/> <a href="#">show interfaces redundancy (Aggregated Ethernet) on page 2161</a><br/> <a href="#">show interfaces redundancy detail on page 2162</a><br/> <a href="#">show interfaces routing brief on page 2162</a><br/> <a href="#">show interfaces routing detail on page 2162</a><br/> <a href="#">show interfaces routing-instance all on page 2163</a><br/> <a href="#">show interfaces snmp-index on page 2163</a><br/> <a href="#">show interfaces source-class all on page 2163</a><br/> <a href="#">show interfaces statistics (Fast Ethernet) on page 2164</a><br/> <a href="#">show interfaces switch-port on page 2164</a><br/> <a href="#">show interfaces transport pm on page 2165</a><br/> <a href="#">show security zones on page 2166</a> </p> |
| <p><b>Output Fields</b></p>         | <p>Table 238 lists the output fields for the <b>show interfaces</b> command. Output fields are listed in the approximate order in which they appear.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 238: show interfaces Output Fields

| Field Name                | Field Description                                                                                                                                                                                                                                   | Level of Output              |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Physical Interface</b> |                                                                                                                                                                                                                                                     |                              |
| <b>Physical interface</b> | Name of the physical interface.                                                                                                                                                                                                                     | All levels                   |
| <b>Enabled</b>            | State of the interface.                                                                                                                                                                                                                             | All levels                   |
| <b>Interface index</b>    | Index number of the physical interface, which reflects its initialization sequence.                                                                                                                                                                 | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | SNMP index number for the physical interface.                                                                                                                                                                                                       | <b>detail extensive none</b> |
| <b>Link-level type</b>    | Encapsulation being used on the physical interface.                                                                                                                                                                                                 | All levels                   |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                   | <b>detail extensive</b>      |
| <b>MTU</b>                | Maximum transmission unit size on the physical interface.                                                                                                                                                                                           | All levels                   |
| <b>Link mode</b>          | Link mode: Full-duplex or Half-duplex.                                                                                                                                                                                                              |                              |
| <b>Speed</b>              | Speed at which the interface is running.                                                                                                                                                                                                            | All levels                   |
| <b>BPDU error</b>         | Bridge protocol data unit (BPDU) error: Detected or None                                                                                                                                                                                            |                              |
| <b>Loopback</b>           | Loopback status: <b>Enabled</b> or <b>Disabled</b> . If loopback is enabled, type of loopback: <b>Local</b> or <b>Remote</b> .                                                                                                                      | All levels                   |
| <b>Source filtering</b>   | Source filtering status: <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                        | All levels                   |
| <b>Flow control</b>       | Flow control status: <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                            | All levels                   |
| <b>Auto-negotiation</b>   | (Gigabit Ethernet interfaces) Autonegotiation status: <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                           | All levels                   |
| <b>Remote-fault</b>       | (Gigabit Ethernet interfaces) Remote fault status: <ul style="list-style-type: none"> <li>• <b>Online</b>—Autonegotiation is manually configured as online.</li> <li>• <b>Offline</b>—Autonegotiation is manually configured as offline.</li> </ul> | All levels                   |
| <b>Device flags</b>       | Information about the physical device.                                                                                                                                                                                                              | All levels                   |
| <b>Interface flags</b>    | Information about the interface.                                                                                                                                                                                                                    | All levels                   |
| <b>Link flags</b>         | Information about the physical link.                                                                                                                                                                                                                | All levels                   |
| <b>CoS queues</b>         | Number of CoS queues configured.                                                                                                                                                                                                                    | <b>detail extensive none</b> |
| <b>Current address</b>    | Configured MAC address.                                                                                                                                                                                                                             | <b>detail extensive none</b> |

Table 238: show interfaces Output Fields (*continued*)

| Field Name                              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Level of Output              |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Last flapped</b>                     | Date, time, and how long ago the interface went from down to up. The format is <b>Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago)</b> . For example, <b>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</b> .                                                                                                                                                                                                                                                                          | <b>detail extensive none</b> |
| <b>Input Rate</b>                       | Input rate in bits per second (bps) and packets per second (pps).                                                                                                                                                                                                                                                                                                                                                                                                                                                             | None                         |
| <b>Output Rate</b>                      | Output rate in bps and pps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | None                         |
| <b>Active alarms and Active defects</b> | <p>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. These fields can contain the value <b>None</b> or <b>Link</b>.</p> <ul style="list-style-type: none"> <li>• <b>None</b>—There are no active defects or alarms.</li> <li>• <b>Link</b>—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</li> </ul> | <b>detail extensive none</b> |
| <b>Statistics last cleared</b>          | Time when the statistics for the interface were last set to zero.                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>detail extensive</b>      |
| <b>Traffic statistics</b>               | <p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received on the interface.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted on the interface.</li> <li>• <b>Input packets</b>—Number of packets received on the interface.</li> <li>• <b>Output packets</b>—Number of packets transmitted on the interface.</li> </ul>                                                                  | <b>detail extensive</b>      |

Table 238: show interfaces Output Fields (*continued*)

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output  |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>Input errors</b>  | <p>Input errors on the interface.</p> <ul style="list-style-type: none"> <li>• <b>Errors</b>—Sum of the incoming frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Number of frames received that are smaller than the runt threshold.</li> <li>• <b>Policed discards</b>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</li> <li>• <b>L3 incompletes</b>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <b>ignore-l3-incompletes</b> statement.</li> <li>• <b>L2 channel errors</b>—Number of times the software did not find a valid logical interface for an incoming frame.</li> <li>• <b>L2 mismatch timeouts</b>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</li> <li>• <b>FIFO errors</b>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>                                                                                                                                                    | <b>extensive</b> |
| <b>Output errors</b> | <p>Output errors on the interface.</p> <ul style="list-style-type: none"> <li>• <b>Carrier transitions</b>—Number of times the interface has gone from <b>down</b> to <b>up</b>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</li> <li>• <b>Errors</b>—Sum of the outgoing frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</li> <li>• <b>Collisions</b>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</li> <li>• <b>Aged packets</b>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</li> <li>• <b>FIFO errors</b>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</li> <li>• <b>HS link CRC errors</b>—Number of errors on the high-speed links between the ASICs responsible for handling the interfaces.</li> <li>• <b>MTU errors</b>—Number of packets whose size exceeded the MTU of the interface.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul> | <b>extensive</b> |

Table 238: show interfaces Output Fields (*continued*)

| Field Name                             | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Level of Output         |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Ingress queues</b>                  | Total number of ingress queues supported on the specified interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>extensive</b>        |
| <b>Queue counters and queue number</b> | CoS queue number and its associated user-configured forwarding class name. <ul style="list-style-type: none"> <li>• <b>Queued packets</b>—Number of queued packets.</li> <li>• <b>Transmitted packets</b>—Number of transmitted packets.</li> <li>• <b>Dropped packets</b>—Number of packets dropped by the ASIC's RED mechanism.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive</b> |
| <b>MAC statistics</b>                  | <p>Receive and Transmit statistics reported by the PIC's MAC subsystem, including the following:</p> <ul style="list-style-type: none"> <li>• <b>Total octets and total packets</b>—Total number of octets and packets.</li> <li>• <b>Unicast packets, Broadcast packets, and Multicast packets</b>—Number of unicast, broadcast, and multicast packets.</li> <li>• <b>CRC/Align errors</b>—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</li> <li>• <b>FIFO error</b>—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</li> <li>• <b>MAC control frames</b>—Number of MAC control frames.</li> <li>• <b>MAC pause frames</b>—Number of MAC control frames with <b>pause</b> operational code.</li> <li>• <b>Oversized frames</b>—There are two possible conditions regarding the number of oversized frames: <ul style="list-style-type: none"> <li>• Packet length exceeds 1518 octets, or</li> <li>• Packet length exceeds MRU</li> </ul> </li> <li>• <b>Jabber frames</b>—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</li> <li>• <b>Fragment frames</b>—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</li> <li>• <b>VLAN tagged frames</b>—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</li> <li>• <b>Code violations</b>—Number of times an event caused the PHY to indicate "Data reception error" or "invalid data symbol error."</li> </ul> | <b>extensive</b>        |

Table 238: show interfaces Output Fields (*continued*)

| Field Name                             | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Level of Output |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Filter statistics                      | <p>Receive and Transmit statistics reported by the PIC's MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet's source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</p> <ul style="list-style-type: none"> <li>• <b>Input packet count</b>—Number of packets received from the MAC hardware that the filter processed.</li> <li>• <b>Input packet rejects</b>—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</li> <li>• <b>Input DA rejects</b>—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local device (which the router is rejecting).</li> <li>• <b>Input SA rejects</b>—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</li> <li>• <b>Output packet count</b>—Number of packets that the filter has given to the MAC hardware.</li> <li>• <b>Output packet pad count</b>—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</li> <li>• <b>Output packet error count</b>—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.</li> <li>• <b>CAM destination filters, CAM source filters</b>—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0.</li> </ul> | extensive       |
| Autonegotiation information            | <p>Information about link autonegotiation.</p> <ul style="list-style-type: none"> <li>• <b>Negotiation status:</b> <ul style="list-style-type: none"> <li>• <b>Incomplete</b>—Ethernet interface has the speed or link mode configured.</li> <li>• <b>No autonegotiation</b>—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.</li> <li>• <b>Complete</b>—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | extensive       |
| Packet Forwarding Engine configuration | <p>Information about the configuration of the Packet Forwarding Engine:</p> <ul style="list-style-type: none"> <li>• <b>Destination slot</b>—FPC slot number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | extensive       |



Table 238: show interfaces Output Fields (*continued*)

| Field Name                           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Level of Output              |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>CoS information</b>               | Information about the CoS queue for the physical interface. <ul style="list-style-type: none"> <li>• <b>CoS transmit queue</b>—Queue number and its associated user-configured forwarding class name.</li> <li>• <b>Bandwidth %</b>—Percentage of bandwidth allocated to the queue.</li> <li>• <b>Bandwidth bps</b>—Bandwidth allocated to the queue (in bps).</li> <li>• <b>Buffer %</b>—Percentage of buffer space allocated to the queue.</li> <li>• <b>Buffer usec</b>—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</li> <li>• <b>Priority</b>—Queue priority: <b>low</b> or <b>high</b>.</li> <li>• <b>Limit</b>—Displayed if rate limiting is configured for the queue. Possible values are <b>none</b> and <b>exact</b>. If <b>exact</b> is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If <b>none</b> is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</li> </ul> | <b>extensive</b>             |
| <b>Interface transmit statistics</b> | Status of the <b>interface-transmit-statistics</b> configuration: Enabled or Disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail extensive</b>      |
| <b>Queue counters (Egress)</b>       | CoS queue number and its associated user-configured forwarding class name. <ul style="list-style-type: none"> <li>• <b>Queued packets</b>—Number of queued packets.</li> <li>• <b>Transmitted packets</b>—Number of transmitted packets.</li> <li>• <b>Dropped packets</b>—Number of packets dropped by the ASIC's RED mechanism.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>detail extensive</b>      |
| <b>Logical Interface</b>             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                              |
| <b>Logical interface</b>             | Name of the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | All levels                   |
| <b>Index</b>                         | Index number of the logical interface, which reflects its initialization sequence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>                  | SNMP interface index number for the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail extensive none</b> |
| <b>Generation</b>                    | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>detail extensive</b>      |
| <b>Flags</b>                         | Information about the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels                   |
| <b>Encapsulation</b>                 | Encapsulation on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | All levels                   |
| <b>Traffic statistics</b>            | Number and rate of bytes and packets received and transmitted on the specified interface set. <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface set.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail extensive</b>      |

Table 238: show interfaces Output Fields (*continued*)

| Field Name                                            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Level of Output              |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Local statistics</b>                               | Number and rate of bytes and packets destined to the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>extensive</b>             |
| <b>Transit statistics</b>                             | Number and rate of bytes and packets transiting the switch.<br><br><b>NOTE:</b> For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the <b>Output bytes</b> and <b>Output packets</b> interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler. | <b>extensive</b>             |
| <b>Security</b>                                       | Security zones that interface belongs to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>extensive</b>             |
| <b>Flow Input statistics</b>                          | Statistics on packets received by flow module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>extensive</b>             |
| <b>Flow Output statistics</b>                         | Statistics on packets sent by flow module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>extensive</b>             |
| <b>Flow error statistics (Packets dropped due to)</b> | Statistics on errors in the flow module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>extensive</b>             |
| <b>Protocol</b>                                       | Protocol family.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>detail extensive none</b> |
| <b>MTU</b>                                            | Maximum transmission unit size on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail extensive none</b> |
| <b>Generation</b>                                     | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail extensive</b>      |
| <b>Route Table</b>                                    | Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail extensive none</b> |
| <b>Flags</b>                                          | Information about protocol family flags. .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>detail extensive</b>      |
| <b>Addresses, Flags</b>                               | Information about the address flags..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>detail extensive none</b> |
| <b>Destination</b>                                    | IP address of the remote side of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>detail extensive none</b> |
| <b>Local</b>                                          | IP address of the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>detail extensive none</b> |
| <b>Broadcast</b>                                      | Broadcast address of the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail extensive none</b> |
| <b>Generation</b>                                     | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail extensive</b>      |

## Sample Output

### show interfaces Gigabit Ethernet

```
user@host> show interfaces ge-0/0/1
```

```

Physical interface: ge-0/0/1, Enabled, Physical link is Down
 Interface index: 135, SNMP ifIndex: 510
 Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,

 BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
 Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
 Remote fault: Online
 Device flags : Present Running Down
 Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
 Link flags : None
 CoS queues : 8 supported, 8 maximum usable queues
 Current address: 00:1f:12:e4:b1:01, Hardware address: 00:1f:12:e4:b1:01
 Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:42 ago)
 Input rate : 0 bps (0 pps)
 Output rate : 0 bps (0 pps)
 Active alarms : LINK
 Active defects : LINK
 Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514)
 Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
 Input packets : 0
 Output packets: 0
 Security: Zone: public
 Protocol inet, MTU: 1500
 Flags: Sendbroadcast-pkt-to-re
 Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
 Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255

```

## Sample Output

### show interfaces brief (Gigabit Ethernet)

```

user@host> show interfaces ge-3/0/2 brief
Physical interface: ge-3/0/2, Enabled, Physical link is Up
 Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
 Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
 Remote fault: Online
 Device flags : Present Running
 Interface flags: SNMP-Traps Internal: 0x4000
 Link flags : None

Logical interface ge-3/0/2.0
 Flags: SNMP-Traps 0x4000
 VLAN-Tag [0x8100.512 0x8100.513] In(pop-swap 0x8100.530) Out(swap-push
 0x8100.512 0x8100.513)
 Encapsulation: VLAN-CCC
 ccc

Logical interface ge-3/0/2.32767
 Flags: SNMP-Traps 0x4000 VLAN-Tag [0x0000.0] Encapsulation: ENET2

```

## Sample Output

### show interfaces detail (Gigabit Ethernet)

```

user@host> show interfaces ge-0/0/1 detail
Physical interface: ge-0/0/1, Enabled, Physical link is Down
 Interface index: 135, SNMP ifIndex: 510, Generation: 138
 Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
 BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering:

```

```

Disabled,
Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:1f:12:e4:b1:01, Hardware address: 00:1f:12:e4:b1:01
Last flapped : 2015-05-12 08:36:59 UTC (1w2d 00:00 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets

0 best-effort 0 0 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 0 0 0

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
Active alarms : LINK
Active defects : LINK
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Security: Zone: public
Flow Statistics :
Flow Input statistics :
Self packets : 0
ICMP packets : 0
VPN packets : 0
Multicast packets : 0
Bytes permitted by policy : 0
Connections established : 0

```

```

Flow Output statistics:
 Multicast packets : 0
 Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
 Address spoofing: 0
 Authentication failed: 0
 Incoming NAT errors: 0
 Invalid zone received packet: 0
 Multiple user authentications: 0
 Multiple incoming NAT: 0
 No parent for a gate: 0
 No one interested in self packets: 0
 No minor session: 0
 No more sessions: 0
 No NAT gate: 0
 No route present: 0
 No SA for incoming SPI: 0
 No tunnel found: 0
 No session for a gate: 0
 No zone or NULL zone binding 0
 Policy denied: 0
 Security association not active: 0
 TCP sequence number out of window: 0
 Syn-attack protection: 0
 User authentication errors: 0
Protocol inet, MTU: 1500, Generation: 150, Route table: 0
 Flags: Sendbroadcast-pkt-to-re
 Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
 Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255, Generation:
150

```

## Sample Output

### show interfaces extensive (Gigabit Ethernet)

```

user@host> show interfaces ge-0/0/1.0 extensive
Physical interface: ge-0/0/1, Enabled, Physical link is Down
 Interface index: 135, SNMP ifIndex: 510, Generation: 138
 Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,

 BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
 Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
 Remote fault: Online
 Device flags : Present Running Down
 Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
 Link flags : None
 CoS queues : 8 supported, 8 maximum usable queues
 Hold-times : Up 0 ms, Down 0 ms
 Current address: 00:1f:12:e4:b1:01, Hardware address: 00:1f:12:e4:b1:01
 Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:57 ago)
 Statistics last cleared: Never
Traffic statistics:
 Input bytes : 0 0 bps
 Output bytes : 0 0 bps
 Input packets: 0 0 pps
 Output packets: 0 0 pps
Input errors:
 Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
 L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
 FIFO errors: 0, Resource errors: 0
Output errors:

```

Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use

Queue counters:            Queued packets    Transmitted packets            Dropped packets

0 best-effort                            0                            0                            0

1 expedited-fo                            0                            0                            0

2 assured-forw                            0                            0                            0

3 network-cont                            0                            0                            0

Queue number:            Mapped forwarding classes

0                            best-effort

1                            expedited-forwarding

2                            assured-forwarding

3                            network-control

Active alarms : LINK

Active defects : LINK

MAC statistics:

Receive

Transmit

Total octets                            0                            0

Total packets                            0                            0

Unicast packets                            0                            0

Broadcast packets                            0                            0

Multicast packets                            0                            0

CRC/Align errors                            0                            0

FIFO errors                            0                            0

MAC control frames                            0                            0

MAC pause frames                            0                            0

Oversized frames                            0

Jabber frames                            0

Fragment frames                            0

VLAN tagged frames                            0

Code violations                            0

Filter statistics:

Input packet count                            0

Input packet rejects                            0

Input DA rejects                            0

Input SA rejects                            0

Output packet count                            0

Output packet pad count                            0

Output packet error count                            0

CAM destination filters: 2, CAM source filters: 0

Autonegotiation information:

Negotiation status: Incomplete

Packet Forwarding Engine configuration:

Destination slot: 0

CoS information:

Direction : Output

CoS transmit queue

Bandwidth

Buffer Priority

Limit

|               | %  | bps       | %  | usec |     |
|---------------|----|-----------|----|------|-----|
| 0 best-effort | 95 | 950000000 | 95 | 0    | low |

none

|                   |   |          |   |   |     |
|-------------------|---|----------|---|---|-----|
| 3 network-control | 5 | 50000000 | 5 | 0 | low |
|-------------------|---|----------|---|---|-----|

none

Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)

```

Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
Local statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
Transit statistics:
 Input bytes : 0 0 bps
 Output bytes : 0 0 bps
 Input packets: 0 0 pps
 Output packets: 0 0 pps
Security: Zone: public
Flow Statistics :
Flow Input statistics :
 Self packets : 0
 ICMP packets : 0
 VPN packets : 0
 Multicast packets : 0
 Bytes permitted by policy : 0
 Connections established : 0
Flow Output statistics:
 Multicast packets : 0
 Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
 Address spoofing: 0
 Authentication failed: 0
 Incoming NAT errors: 0
 Invalid zone received packet: 0
 Multiple user authentications: 0
 Multiple incoming NAT: 0
 No parent for a gate: 0
 No one interested in self packets: 0
 No minor session: 0
 No more sessions: 0
 No NAT gate: 0
 No route present: 0
 No SA for incoming SPI: 0
 No tunnel found: 0
 No session for a gate: 0
 No zone or NULL zone binding: 0
 Policy denied: 0
 Security association not active: 0
 TCP sequence number out of window: 0
 Syn-attack protection: 0
 User authentication errors: 0
Protocol inet, MTU: 1500, Generation: 150, Route table: 0
Flags: Sendbcst-pkt-to-re
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
 Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255,
 Generation: 150

```

## Sample Output

### show interfaces terse

```

user@host> show interfaces terse

```

| Interface      | Admin | Link  | Proto | Local                 | Remote             |
|----------------|-------|-------|-------|-----------------------|--------------------|
| ge-0/0/0       | up    | up    |       |                       |                    |
| ge-0/0/0.0     | up    | up    | inet  | 10.209.4.61/18        |                    |
| gr-0/0/0       | up    | up    |       |                       |                    |
| ip-0/0/0       | up    | up    |       |                       |                    |
| st0            | up    | up    |       |                       |                    |
| st0.1          | up    | ready | inet  |                       |                    |
| ls-0/0/0       | up    | up    |       |                       |                    |
| lt-0/0/0       | up    | up    |       |                       |                    |
| mt-0/0/0       | up    | up    |       |                       |                    |
| pd-0/0/0       | up    | up    |       |                       |                    |
| pe-0/0/0       | up    | up    |       |                       |                    |
| e3-1/0/0       | up    | up    |       |                       |                    |
| t3-2/0/0       | up    | up    |       |                       |                    |
| e1-3/0/0       | up    | up    |       |                       |                    |
| se-4/0/0       | up    | down  |       |                       |                    |
| t1-5/0/0       | up    | up    |       |                       |                    |
| br-6/0/0       | up    | up    |       |                       |                    |
| dc-6/0/0       | up    | up    |       |                       |                    |
| dc-6/0/0.32767 | up    | up    |       |                       |                    |
| bc-6/0/0:1     | down  | up    |       |                       |                    |
| bc-6/0/0:1.0   | up    | down  |       |                       |                    |
| d10            | up    | up    |       |                       |                    |
| d10.0          | up    | up    | inet  |                       |                    |
| dsc            | up    | up    |       |                       |                    |
| gre            | up    | up    |       |                       |                    |
| ipip           | up    | up    |       |                       |                    |
| lo0            | up    | up    |       |                       |                    |
| lo0.16385      | up    | up    | inet  | 10.0.0.1<br>10.0.0.16 | --> 0/0<br>--> 0/0 |
| lsi            | up    | up    |       |                       |                    |
| mtun           | up    | up    |       |                       |                    |
| pimd           | up    | up    |       |                       |                    |
| pime           | up    | up    |       |                       |                    |
| pp0            | up    | up    |       |                       |                    |

## Sample Output

### show interfaces controller (Channelized E1 IQ with Logical E1)

```

user@host> show interfaces controller ce1-1/2/6

```

| Controller | Admin | Link |
|------------|-------|------|
| ce1-1/2/6  | up    | up   |
| e1-1/2/6   | up    | up   |

### show interfaces controller (Channelized E1 IQ with Logical DSO)

```

user@host> show interfaces controller ce1-1/2/3

```

| Controller | Admin | Link |
|------------|-------|------|
| ce1-1/2/3  | up    | up   |
| ds-1/2/3:1 | up    | up   |
| ds-1/2/3:2 | up    | up   |



## Sample Output

### show interfaces descriptions

```

user@host> show interfaces descriptions
Interface Admin Link Description
so-1/0/0 up up M20-3#1
so-2/0/0 up up GSR-12#1
ge-3/0/0 up up SMB-OSPF_Area300
so-3/3/0 up up GSR-13#1
so-3/3/1 up up GSR-13#2
ge-4/0/0 up up T320-7#1
ge-5/0/0 up up T320-7#2
so-7/1/0 up up M160-6#1
ge-8/0/0 up up T320-7#3
ge-9/0/0 up up T320-7#4
so-10/0/0 up up M160-6#2
so-13/0/0 up up M20-3#2
so-14/0/0 up up GSR-12#2
ge-15/0/0 up up SMB-OSPF_Area100
ge-15/0/1 up up GSR-13#3

```

## Sample Output

### show interfaces destination-class all

```

user@host> show interfaces destination-class all
Logical interface so-4/0/0.0

 Destination class Packets Bytes
 (packet-per-second) (bits-per-second)
 gold 0 0
 (0) (0)
 silver 0 0
 (0) (0)
Logical interface so-0/1/3.0

 Destination class Packets Bytes
 (packet-per-second) (bits-per-second)
 gold 0 0
 (0) (0)
 silver 0 0
 (0) (0)

```

## Sample Output

### show interfaces diagnostics optics

```

user@host> show interfaces diagnostics optics ge-2/0/0
Physical interface: ge-2/0/0
Laser bias current : 7.408 mA
Laser output power : 0.3500 mW / -4.56 dBm
Module temperature : 23 degrees C / 73 degrees F
Module voltage : 3.3450 V
Receiver signal average optical power : 0.0002 mW / -36.99 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off

```

```

Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : On
Laser rx power high warning : Off
Laser rx power low warning : On
Laser bias current high alarm threshold : 17.000 mA
Laser bias current low alarm threshold : 1.000 mA
Laser bias current high warning threshold : 14.000 mA
Laser bias current low warning threshold : 2.000 mA
Laser output power high alarm threshold : 0.6310 mW / -2.00 dBm
Laser output power low alarm threshold : 0.0670 mW / -11.74 dBm
Laser output power high warning threshold : 0.6310 mW / -2.00 dBm
Laser output power low warning threshold : 0.0790 mW / -11.02 dBm
Module temperature high alarm threshold : 95 degrees C / 203 degrees F
Module temperature low alarm threshold : -25 degrees C / -13 degrees F
Module temperature high warning threshold : 90 degrees C / 194 degrees F
Module temperature low warning threshold : -20 degrees C / -4 degrees F
Module voltage high alarm threshold : 3.900 V
Module voltage low alarm threshold : 2.700 V
Module voltage high warning threshold : 3.700 V
Module voltage low warning threshold : 2.900 V
Laser rx power high alarm threshold : 1.2590 mW / 1.00 dBm
Laser rx power low alarm threshold : 0.0100 mW / -20.00 dBm
Laser rx power high warning threshold : 0.7940 mW / -1.00 dBm
Laser rx power low warning threshold : 0.0158 mW / -18.01 dBm

```

## Sample Output

### show interfaces far-end-interval coc12-5/2/0

```

user@host> show interfaces far-end-interval coc12-5/2/0
Physical interface: coc12-5/2/0, SNMP ifIndex: 121
05:30-current:
 ES-L: 1, SES-L: 1, UAS-L: 0
05:15-05:30:
 ES-L: 0, SES-L: 0, UAS-L: 0
05:00-05:15:
 ES-L: 0, SES-L: 0, UAS-L: 0
04:45-05:00:
 ES-L: 0, SES-L: 0, UAS-L: 0
04:30-04:45:
 ES-L: 0, SES-L: 0, UAS-L: 0
04:15-04:30:
 ES-L: 0, SES-L: 0, UAS-L: 0
04:00-04:15:
...

```

### show interfaces far-end-interval coc1-5/2/1:1

```

user@host> run show interfaces far-end-interval coc1-5/2/1:1
Physical interface: coc1-5/2/1:1, SNMP ifIndex: 342
05:30-current:
 ES-L: 1, SES-L: 1, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0

```

```

05:15-05:30:
 ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
05:00-05:15:
 ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:45-05:00:
 ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:30-04:45:
 ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:15-04:30:
 ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:00-04:15:

```

## Sample Output

### show interfaces filters

```

user@host> show interfaces filters
Interface Admin Link Proto Input Filter Output Filter
ge-0/0/0 up up inet
ge-0/0/0.0 up up inet
 iso
ge-5/0/0 up up
ge-5/0/0.0 up up any f-any
 inet f-inet
 multiservice
gr-0/3/0 up up
ip-0/3/0 up up
mt-0/3/0 up up
pd-0/3/0 up up
pe-0/3/0 up up
vt-0/3/0 up up
at-1/0/0 up up
at-1/0/0.0 up up inet
 iso
at-1/1/0 up down
at-1/1/0.0 up down inet
 iso
....

```

## Sample Output

### show interfaces flow-statistics (Gigabit Ethernet)

```

user@host> show interfaces flow-statistics ge-0/0/1.0
Logical interface ge-0/0/1.0 (Index 70) (SNMP ifIndex 49)
Flags: SNMP-Traps Encapsulation: ENET2
Input packets : 5161
Output packets: 83
Security: Zone: zone2
Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm
pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset http
https ike
netconf ping rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
xnm-ssl
Ispring
Flow Statistics :
Flow Input statistics :
Self packets : 0
ICMP packets : 0
VPN packets : 2564

```

```

Bytes permitted by policy : 3478
Connections established : 1
Flow Output statistics:
Multicast packets : 0
Bytes permitted by policy : 16994
Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0
Protocol inet, MTU: 1500
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113.1/24, Local: 203.0.113.2, Broadcast: 2.2.2.255

```

## Sample Output

### show interfaces interval (Channelized OC12)

```

user@host> show interfaces interval t3-0/3/0:0
Physical interface: t3-0/3/0:0, SNMP ifIndex: 23
17:43-current:
LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
SEFS: 0, UAS: 0
17:28-17:43:
LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
SEFS: 0, UAS: 0
17:13-17:28:
LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
SEFS: 0, UAS: 0
16:58-17:13:
LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
SEFS: 0, UAS: 0
16:43-16:58:
LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
...
Interval Total:
LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,
CES: 230, CSES: 230, SEFS: 230, UAS: 238

```

### show interfaces interval (E3)

```

user@host> show interfaces interval e3-0/3/0

```

```

Physical interface: e3-0/3/0, SNMP ifIndex: 23
17:43-current:
 LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
 SEFS: 0, UAS: 0
17:28-17:43:
 LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
 SEFS: 0, UAS: 0
17:13-17:28:
 LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
 SEFS: 0, UAS: 0
16:58-17:13:
 LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
 SEFS: 0, UAS: 0
16:43-16:58:
 LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,

Interval Total:
 LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,
 CES: 230, CSES: 230, SEFS: 230, UAS: 238

```

### show interfaces interval (SONET/SDH)

```

user@host> show interfaces interval so-0/1/0
Physical interface: so-0/1/0, SNMP ifIndex: 19
20:02-current:
 ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0,
 SES-P: 0, UAS-P: 0
19:47-20:02:
 ES-S: 267, SES-S: 267, SEFS-S: 267, ES-L: 267, SES-L: 267, UAS-L: 267,
 ES-P: 267, SES-P: 267, UAS-P: 267
19:32-19:47:
 ES-S: 56, SES-S: 56, SEFS-S: 56, ES-L: 56, SES-L: 56, UAS-L: 46, ES-P: 56,
 SES-P: 56, UAS-P: 46
19:17-19:32:
 ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0,
 SES-P: 0, UAS-P: 0
19:02-19:17:


```

## Sample Output

### show interfaces load-balancing

```

user@host> show interfaces load-balancing
Interface State Last change Member count
ams0 Up 1d 00:50 2
ams1 Up 00:00:59 2

```

### show interfaces load-balancing detail

```

user@host> show interfaces load-balancing detail
Load-balancing interfaces detail
Interface : ams0
State : Up
Last change : 1d 00:51
Member count : 2
Members :
 Interface Weight State
 mams-2/0/0 10 Active
 mams-2/1/0 10 Active

```

## Sample Output

### show interfaces mac-database (All MAC Addresses on a Port)

```

user@host> show interfaces mac-database xe-0/3/3
Physical interface: xe-0/3/3, Enabled, Physical link is Up
 Interface index: 372, SNMP ifIndex: 788
 Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, Loopback:
None, Source filtering: Disabled, Flow control: Enabled
 Device flags : Present Running
 Interface flags: SNMP-Traps Internal: 0x4000
 Link flags : None

Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
 Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2

```

| MAC address       | Input frames | Input bytes | Output frames | Output bytes |
|-------------------|--------------|-------------|---------------|--------------|
| 00:00:00:00:00:00 | 1            | 56          | 0             | 0            |
| 00:00:c0:01:01:02 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:03 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:04 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:05 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:06 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:07 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:08 | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:09 | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:0a | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:0b | 7023809      | 323095214   | 0             | 0            |
| 00:00:c8:01:01:02 | 30424784     | 1399540064  | 37448598      | 1722635508   |
| 00:00:c8:01:01:03 | 30424784     | 1399540064  | 37448598      | 1722635508   |
| 00:00:c8:01:01:04 | 30424716     | 1399536936  | 37448523      | 1722632058   |
| 00:00:c8:01:01:05 | 30424789     | 1399540294  | 37448598      | 1722635508   |
| 00:00:c8:01:01:06 | 30424788     | 1399540248  | 37448597      | 1722635462   |
| 00:00:c8:01:01:07 | 30424783     | 1399540018  | 37448597      | 1722635462   |
| 00:00:c8:01:01:08 | 30424783     | 1399540018  | 37448596      | 1722635416   |
| 00:00:c8:01:01:09 | 8836796      | 406492616   | 8836795       | 406492570    |
| 00:00:c8:01:01:0a | 30424712     | 1399536752  | 37448521      | 1722631966   |
| 00:00:c8:01:01:0b | 30424715     | 1399536890  | 37448523      | 1722632058   |

Number of MAC addresses : 21

### show interfaces mac-database (All MAC Addresses on a Service)

```

user@host> show interfaces mac-database xe-0/3/3
Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
 Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2

```

| MAC address       | Input frames | Input bytes | Output frames | Output bytes |
|-------------------|--------------|-------------|---------------|--------------|
| 00:00:00:00:00:00 | 1            | 56          | 0             | 0            |
| 00:00:c0:01:01:02 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:03 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:04 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:05 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:06 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:07 | 7023810      | 323095260   | 0             | 0            |
| 00:00:c0:01:01:08 | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:09 | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:0a | 7023809      | 323095214   | 0             | 0            |
| 00:00:c0:01:01:0b | 7023809      | 323095214   | 0             | 0            |
| 00:00:c8:01:01:02 | 31016568     | 1426762128  | 38040381      | 1749857526   |

|                   |          |            |          |            |
|-------------------|----------|------------|----------|------------|
| 00:00:c8:01:01:03 | 31016568 | 1426762128 | 38040382 | 1749857572 |
| 00:00:c8:01:01:04 | 31016499 | 1426758954 | 38040306 | 1749854076 |
| 00:00:c8:01:01:05 | 31016573 | 1426762358 | 38040381 | 1749857526 |
| 00:00:c8:01:01:06 | 31016573 | 1426762358 | 38040381 | 1749857526 |
| 00:00:c8:01:01:07 | 31016567 | 1426762082 | 38040380 | 1749857480 |
| 00:00:c8:01:01:08 | 31016567 | 1426762082 | 38040379 | 1749857434 |
| 00:00:c8:01:01:09 | 9428580  | 433714680  | 9428580  | 433714680  |
| 00:00:c8:01:01:0a | 31016496 | 1426758816 | 38040304 | 1749853984 |
| 00:00:c8:01:01:0b | 31016498 | 1426758908 | 38040307 | 1749854122 |

### show interfaces mac-database mac-address

```

user@host> show interfaces mac-database xe-0/3/3 mac-address 00:00:c8:01:01:09
Physical interface: xe-0/3/3, Enabled, Physical link is Up
 Interface index: 372, SNMP ifIndex: 788
 Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, Loopback:
None, Source filtering: Disabled, Flow control: Enabled
 Device flags : Present Running
 Interface flags: SNMP-Traps Internal: 0x4000
 Link flags : None

 Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
 Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
 MAC address: 00:00:c8:01:01:09, Type: Configured,
 Input bytes : 202324652
 Output bytes : 202324560
 Input frames : 4398362
 Output frames : 4398360
 Policer statistics:
 Policer type Discarded frames Discarded bytes
 Output aggregate 3992386 183649756

```

## Sample Output

### show interfaces mc-ae

```

user@host> show interfaces mc-ae ae0 unit 512
Member Links : ae0
Local Status : active
Peer Status : active
Logical Interface : ae0.512
Core Facing Interface : Label Ethernet Interface
ICL-PL : Label Ethernet Interface

```

### show interfaces media (SONET/SDH)

The following example displays the output fields unique to the **show interfaces media** command for a SONET interface (with no level of output specified):

```

user@host> show interfaces media so-4/1/2
Physical interface: so-4/1/2, Enabled, Physical link is Up
 Interface index: 168, SNMP ifIndex: 495
 Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
Loopback: None, FCS: 16, Payload scrambler: Enabled
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps 16384
 Link flags : Keepalives
 Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
 Keepalive: Input: 1783 (00:00:00 ago), Output: 1786 (00:00:08 ago)
 LCP state: Opened

```

```

NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Not-configured
CoS queues : 8 supported
Last flapped : 2005-06-15 12:14:59 PDT (04:31:29 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : None
SONET defects : None
SONET errors:
 BIP-B1: 121, BIP-B2: 916, REI-L: 0, BIP-B3: 137, REI-P: 16747, BIP-BIP2: 0
Received path trace: routerb so-1/1/2
Transmitted path trace: routera so-4/1/2

```

## Sample Output

### show interfaces policers

```

user@host> show interfaces policers
Interface Admin Link Proto Input Policer Output Policer
ge-0/0/0 up up inet
ge-0/0/0.0 up up inet
 iso
gr-0/3/0 up up
ip-0/3/0 up up
mt-0/3/0 up up
pd-0/3/0 up up
pe-0/3/0 up up
...
so-2/0/0 up up
so-2/0/0.0 up up inet so-2/0/0.0-in-policer so-2/0/0.0-out-policer
 iso
so-2/1/0 up down
...

```

### show interfaces policers interface-name

```

user@host> show interfaces policers so-2/1/0
Interface Admin Link Proto Input Policer Output Policer
so-2/1/0 up down
so-2/1/0.0 up down inet so-2/1/0.0-in-policer so-2/1/0.0-out-policer
 iso
 inet6

```

## Sample Output

### show interfaces queue

The following truncated example shows the CoS queue sizes for queues 0, 1, and 3. Queue 1 has a queue buffer size (guaranteed allocated memory) of 9192 bytes.

```

user@host> show interfaces queue
Physical interface: ge-0/0/0, Enabled, Physical link is Up
 Interface index: 134, SNMP ifIndex: 509
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: class0
 Queued:
 Packets : 0 0 pps
 Bytes : 0 0 bps

```



```

Transmitted:
 Packets : 0 0 pps
 Bytes : 0 0 bps
 Tail-dropped packets : 0 0 pps
 RL-dropped packets : 0 0 pps
 RL-dropped bytes : 0 0 bps
 RED-dropped packets : 0 0 pps
 Low : 0 0 pps
 Medium-low : 0 0 pps
 Medium-high : 0 0 pps
 High : 0 0 pps
 RED-dropped bytes : 0 0 bps
 Low : 0 0 bps
 Medium-low : 0 0 bps
 Medium-high : 0 0 bps
 High : 0 0 bps
Queue Buffer Usage:
 Reserved buffer : 118750000 bytes
 Queue-depth bytes :
 Current : 0
..
..
Queue: 1, Forwarding classes: class1
..
..
Queue Buffer Usage:
 Reserved buffer : 9192 bytes
 Queue-depth bytes :
 Current : 0
..
..
Queue: 3, Forwarding classes: class3
 Queued:
..
..
Queue Buffer Usage:
 Reserved buffer : 62500000 bytes
 Queue-depth bytes :
 Current : 0
..
..

```

## Sample Output

### show interfaces redundancy

```

user@host> show interfaces redundancy
Interface State Last change Primary Secondary Current status
rsp0 Not present
rsp1 On secondary 1d 23:56 sp-1/2/0 sp-0/3/0 primary down
rsp2 On primary 10:10:27 sp-1/3/0 sp-0/2/0 secondary down
rlsq0 On primary 00:06:24 lsq-0/3/0 lsq-1/0/0 both up

```

### show interfaces redundancy (Aggregated Ethernet)

```

user@host> show interfaces redundancy
Interface State Last change Primary Secondary Current status
rlsq0 On secondary 00:56:12 lsq-4/0/0 lsq-3/0/0 both up

ae0
ae1

```

```
ae2
ae3
ae4
```

### show interfaces redundancy detail

```
user@host> show interfaces redundancy detail
Interface : rlsq0
State : On primary
Last change : 00:45:47
Primary : lsq-0/2/0
Secondary : lsq-1/2/0
Current status : both up
Mode : hot-standby

Interface : rlsq0:0
State : On primary
Last change : 00:45:46
Primary : lsq-0/2/0:0
Secondary : lsq-1/2/0:0
Current status : both up
Mode : warm-standby
```

## Sample Output

### show interfaces routing brief

```
user@host> show interfaces routing brief
Interface State Addresses
so-5/0/3.0 Down ISO enabled
so-5/0/2.0 Up MPLS enabled
 ISO enabled
 INET 192.168.2.120
 INET enabled
so-5/0/1.0 Up MPLS enabled
 ISO enabled
 INET 192.168.2.130
 INET enabled
at-1/0/0.3 Up CCC enabled
at-1/0/0.2 Up CCC enabled
at-1/0/0.0 Up ISO enabled
 INET 192.168.90.10
 INET enabled
lo0.0 Up ISO 47.0005.80ff.f800.0000.0108.0001.1921.6800.5061.00
 ISO enabled
 INET 127.0.0.1
fxp1.0 Up
fxp0.0 Up INET 192.168.6.90
```

### show interfaces routing detail

```
user@host> show interfaces routing detail
so-5/0/3.0
 Index: 15, Refcount: 2, State: Up <Broadcast PointToPoint Multicast> Change:<>

 Metric: 0, Up/down transitions: 0, Full-duplex
 Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
 ISO address (null)
 State: <Broadcast PointToPoint Multicast> Change: <>
 Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
so-5/0/2.0
```

```

Index: 14, Refcount: 7, State: <Up Broadcast PointToPoint Multicast> Change:<>

Metric: 0, Up/down transitions: 0, Full-duplex
Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
MPLS address (null)
 State: <Up Broadcast PointToPoint Multicast> Change: <>
 Preference: 0 (120 down), Metric: 0, MTU: 4458 bytes
ISO address (null)
 State: <Up Broadcast PointToPoint Multicast> Change: <>
 Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
INET address 192.168.2.120
 State: <Up Broadcast PointToPoint Multicast Localup> Change: <>
 Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
 Local address: 192.168.2.120
 Destination: 192.168.2.110/32
INET address (null)
 State: <Up Broadcast PointToPoint Multicast> Change: <>
 Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
...

```

## Sample Output

show interfaces routing-instance all

```

user@host> show interfaces terse routing-instance all
Interface Admin Link Proto Local Remote Instance
at-0/0/1 up up inet 10.0.0.1/24
ge-0/0/0.0 up up inet 192.168.4.28/24 sample-a
at-0/1/0.0 up up inet6 fe80::a:0:0:4/64 sample-b
so-0/0/0.0 up up inet 10.0.0.1/32

```

## Sample Output

show interfaces snmp-index

```

user@host> show interfaces snmp-index 33
Physical interface: so-2/1/1, Enabled, Physical link is Down
Interface index: 149, SNMP ifIndex: 33
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
Link flags : Keepalives
CoS queues : 8 supported
Last flapped : 2005-06-15 11:45:57 PDT (05:38:43 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : LOL, PLL, LOS
SONET defects : LOL, PLL, LOF, LOS, SEF, AIS-L, AIS-P

```

## Sample Output

show interfaces source-class all

```

user@host> show interfaces source-class all
Logical interface so-0/1/0.0

Source class Packets Bytes
 (packet-per-second) (bits-per-second)
gold 1928095 161959980
(889) (597762)
bronze 0 0

```

```

 (0) (0)
 silver 0 0
 (0) (0)
Logical interface so-0/1/3.0
 Source class Packets Bytes
 (packet-per-second) (bits-per-second)
 gold 0 0
 (0) (0)
 bronze 0 0
 (0) (0)
 silver 116113 9753492
 (939) (631616)

```

## Sample Output

### show interfaces statistics (Fast Ethernet)

```

user@host> show interfaces fe-1/3/1 statistics
Physical interface: fe-1/3/1, Enabled, Physical link is Up
 Interface index: 144, SNMP ifIndex: 1042
 Description: ford fe-1/3/1
 Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
 Source filtering: Disabled, Flow control: Enabled
 Device flags : Present Running
 Interface flags: SNMP-Traps Internal: 0x4000
 CoS queues : 4 supported, 4 maximum usable queues
 Current address: 00:90:69:93:04:dc, Hardware address: 00:90:69:93:04:dc
 Last flapped : 2006-04-18 03:08:59 PDT (00:01:24 ago)
 Statistics last cleared: Never
 Input rate : 0 bps (0 pps)
 Output rate : 0 bps (0 pps)
 Input errors: 0, Output errors: 0
 Active alarms : None
 Active defects : None
Logical interface fe-1/3/1.0 (Index 69) (SNMP ifIndex 50)
 Flags: SNMP-Traps Encapsulation: ENET2
 Protocol inet, MTU: 1500
 Flags: Is-Primary, DCU, SCU-in
 Destination class Packets Bytes
 (packet-per-second) (bits-per-second)
 silver1 0 0
 (0) (0)
 silver2 0 0
 (0) (0)
 silver3 0 0
 (0) (0)
 Addresses, Flags: Is-Default Is-Preferred Is-Primary
 Destination: 10.27.245/24, Local: 10.27.245.2,
 Broadcast: 10.27.245.255
 Protocol iso, MTU: 1497
 Flags: Is-Primary

```

## Sample Output

### show interfaces switch-port

```

user@host# show interfaces ge-slot/0/0 switch-port port-number
Port 0, Physical link is Up
 Speed: 100mbps, Auto-negotiation: Enabled
 Statistics:
 Total bytes Receive Transmit
 28437086 21792250

```

```

Total packets 409145 88008
Unicast packets 9987 83817
Multicast packets 145002 0
Broadcast packets 254156 4191
Multiple collisions 23 10
FIFO/CRC/Align errors 0 0
MAC pause frames 0 0
Oversized frames 0
Runt frames 0
Jabber frames 0
Fragment frames 0
Discarded frames 0
Autonegotiation information:
Negotiation status: Complete
Link partner:
Link mode: Full-duplex, Flow control: None, Remote fault: OK, Link
partner Speed: 100 Mbps
Local resolution:
Flow control: None, Remote fault: Link OK

```

## Sample Output

### show interfaces transport pm

```

user@host> show interfaces transport pm all current et-0/1/0
Physical interface: et-0/1/0, SNMP ifIndex 515
14:45-current Elapse time:900 Seconds
Near End Suspect Flag:False Reason:None
PM COUNT THRESHOLD TCA-ENABLED TCA-RAISED

OTU-BBE 0 800 No No
OTU-ES 0 135 No No
OTU-SES 0 90 No No
OTU-UAS 427 90 No No
Far End Suspect Flag:True Reason:Unknown
PM COUNT THRESHOLD TCA-ENABLED TCA-RAISED

OTU-BBE 0 800 No No
OTU-ES 0 135 No No
OTU-SES 0 90 No No
OTU-UAS 0 90 No No
Near End Suspect Flag:False Reason:None
PM COUNT THRESHOLD TCA-ENABLED TCA-RAISED

ODU-BBE 0 800 No No
ODU-ES 0 135 No No
ODU-SES 0 90 No No
ODU-UAS 427 90 No No
Far End Suspect Flag:True Reason:Unknown
PM COUNT THRESHOLD TCA-ENABLED TCA-RAISED

ODU-BBE 0 800 No No
ODU-ES 0 135 No No
ODU-SES 0 90 No No
ODU-UAS 0 90 No No
FEC Suspect Flag:False Reason:None
PM COUNT THRESHOLD TCA-ENABLED TCA-RAISED

FEC-CorrectedErr 2008544300 0 NA NA
FEC-UncorrectedWords 0 0 NA NA
BER Suspect Flag:False Reason:None

```

| PM                                             | MIN        | MAX    | AVG    | THRESHOLD | TCA-ENABLED |
|------------------------------------------------|------------|--------|--------|-----------|-------------|
| TCA-RAISED                                     |            |        |        |           |             |
| BER                                            | 3.6e-5     | 5.8e-5 | 3.6e-5 | 10.0e-3   | No          |
| Yes                                            |            |        |        |           |             |
| Physical interface: et-0/1/0, SNMP ifIndex 515 |            |        |        |           |             |
| 14:45-current                                  |            |        |        |           |             |
| Suspect Flag: True Reason: Object Disabled     |            |        |        |           |             |
| PM                                             | CURRENT    | MIN    | MAX    | AVG       | THRESHOLD   |
| TCA-ENABLED                                    | TCA-RAISED |        |        |           |             |
| (MAX)                                          | (MIN)      | (MAX)  | (MIN)  | (MAX)     | (MIN)       |
| Lane chromatic dispersion                      | 0          | 0      | 0      | 0         | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| Lane differential group delay                  | 0          | 0      | 0      | 0         | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| q Value                                        | 120        | 120    | 120    | 120       | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| SNR                                            | 28         | 28     | 29     | 28        | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| Tx output power(0.01dBm)                       | -5000      | -5000  | -5000  | -5000     | -300        |
| -100 No No No No                               |            |        |        |           |             |
| Rx input power(0.01dBm)                        | -3642      | -3665  | -3626  | -3637     | -1800       |
| -500 No No No No                               |            |        |        |           |             |
| Module temperature(Celsius)                    | 46         | 46     | 46     | 46        | -5          |
| 75 No No No No                                 |            |        |        |           |             |
| Tx laser bias current(0.1mA)                   | 0          | 0      | 0      | 0         | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| Rx laser bias current(0.1mA)                   | 1270       | 1270   | 1270   | 1270      | 0           |
| 0 NA NA NA NA                                  |            |        |        |           |             |
| Carrier frequency offset(MHz)                  | -186       | -186   | -186   | -186      | -5000       |
| 5000 No No No No                               |            |        |        |           |             |

## Sample Output

### show security zones

```

user@host> show security zones
Functional zone: management
 Description: This is the management zone.
 Policy configurable: No
 Interfaces bound: 1
 Interfaces:
 ge-0/0/0.0
Security zone: Host
 Description: This is the host zone.
 Send reset for non-SYN session TCP packets: Off
 Policy configurable: Yes
 Interfaces bound: 1
 Interfaces:
 fxp0.0
Security zone: abc
 Description: This is the abc zone.
 Send reset for non-SYN session TCP packets: Off
 Policy configurable: Yes
 Interfaces bound: 1
 Interfaces:
 ge-0/0/1.0
Security zone: def
 Description: This is the def zone.
 Send reset for non-SYN session TCP packets: Off
 Policy configurable: Yes

```

```
Interfaces bound: 1
Interfaces:
 ge-0/0/2.0
```

## show interfaces snmp-index

---

|                                 |                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show interfaces snmp-index <i>snmp-index</i></code>                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                            |
| <b>Description</b>              | Display information for the interface with the specified SNMP index.                                                                                                                                                                                                       |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                                               |
| <b>Additional Information</b>   | Output from both the <code>show interfaces <i>interface-name</i> detail</code> and the <code>show interfaces <i>interface-name</i> extensive</code> command includes all the information displayed in the output from the <code>show interfaces snmp-index</code> command. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show interfaces snmp-index on page 2168</a>                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | The output fields from the <code>show interfaces snmp-index <i>snmp-index</i></code> command are identical to those produced by the <code>show interfaces <i>interface-name</i></code> command. For a description of output fields, see the other chapters in this manual. |

## Sample Output

### show interfaces snmp-index

```
user@host> show interfaces snmp-index 33
Physical interface: so-2/1/1, Enabled, Physical link is Down
 Interface index: 149, SNMP ifIndex: 33
 Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: 0C48,
 Loopback: None, FCS: 16, Payload scrambler: Enabled
 Device flags : Present Running Down
 Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
 Link flags : Keepalives
 CoS queues : 8 supported
 Last flapped : 2005-06-15 11:45:57 PDT (05:38:43 ago)
 Input rate : 0 bps (0 pps)
 Output rate : 0 bps (0 pps)
 SONET alarms : LOL, PLL, LOS
 SONET defects : LOL, PLL, LOF, LOS, SEF, AIS-L, AIS-P
```



## show interfaces summary

|                                 |                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show interfaces summary</b>                                                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1R2.                                                                                                                |
| <b>Description</b>              | Display the status and statistics on logical interfaces configured on the device at the Flexible PIC Concentrator (FPC) level.                                |
| <b>Options</b>                  | This command has no options.                                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show interfaces summary on page 2169</a>                                                                                                          |
| <b>Output Fields</b>            | Table 239 describes the output fields for the <b>show interfaces summary</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 239: show interfaces summary Output Fields**

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System's maximum logical interfaces | Total number of logical interfaces in the device.                                                                                                                                                                                                                                                                                                                                                                                         |
| Logical interfaces allocated        | Number of allocated logical interfaces.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Logical interfaces available        | Number of available logical interfaces.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Logical interface type              | The type of logical interfaces. <ul style="list-style-type: none"> <li>• <b>LSI</b>—Number of label-switched logical interfaces and their status.</li> <li>• <b>Ethernet Untagged</b>—Number of untagged logical interfaces and their status.</li> <li>• <b>Ethernet VLAN</b>—Number of tagged logical interfaces and their status.</li> <li>• <b>Others</b>—Number of dynamic and other logical interfaces, and their status.</li> </ul> |
| System                              | Statistics on the global logical interfaces in the system.                                                                                                                                                                                                                                                                                                                                                                                |
| FPC x                               | Statistics on the logical interfaces in a specific FPC.                                                                                                                                                                                                                                                                                                                                                                                   |

## Sample Output

### show interfaces summary

```

user@host> show interfaces summary
Logical interfaces:
 System's maximum logical interfaces : 262144
 Logical interfaces allocated : 31
 Logical interfaces available : 262113

System:
Logical interface type Count UP DOWN
Total 28 28 0

```

|                   |    |    |   |
|-------------------|----|----|---|
| LSI               | 0  | 0  | 0 |
| Ethernet Untagged | 15 | 15 | 0 |
| Ethernet VLAN     | 0  | 0  | 0 |
| Others            | 13 | 13 | 0 |

## FPC1:

| Logical interface type | Count | UP | DOWN |
|------------------------|-------|----|------|
| Total                  | 3     | 3  | 0    |
| LSI                    | 0     | 0  | 0    |
| Ethernet Untagged      | 3     | 3  | 0    |
| Ethernet VLAN          | 0     | 0  | 0    |
| Others                 | 0     | 0  | 0    |

## FPC2:

| Logical interface type | Count | UP | DOWN |
|------------------------|-------|----|------|
| Total                  | 0     | 0  | 0    |
| LSI                    | 0     | 0  | 0    |
| Ethernet Untagged      | 0     | 0  | 0    |
| Ethernet VLAN          | 0     | 0  | 0    |
| Others                 | 0     | 0  | 0    |

## show ilmi statistics

---

|                                 |                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show ilmi statistics                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                        |
| <b>Description</b>              | Display input and output Integrated Local Management Interface (ILMI) statistics.                                                                                      |
| <b>Options</b>                  | This command has no options.                                                                                                                                           |
| <b>Required Privilege Level</b> | view                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">clear ilmi statistics on page 2119</a></li></ul>                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show ilmi statistics on page 2173</a>                                                                                                                      |
| <b>Output Fields</b>            | <a href="#">Table 240</a> lists the output fields for the <b>show ilmi statistics</b> command. Output fields are listed in the approximate order in which they appear. |

Table 240: show ilmi statistics Output Fields

| Field Name    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>  | <p>Information about received ILMI packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets</b>—Total number of messages delivered to the ILMI entity from the transport service.</li> <li>• <b>Bad versions</b>—Total number of messages delivered to the ILMI entity that were for an unsupported ILMI version.</li> <li>• <b>Bad community names</b>—Total number of messages delivered to the ILMI entity that did not use an ILMI community name.</li> <li>• <b>Bad community uses</b>—Total number of messages delivered to the ILMI entity that represented an ILMI operation that was not allowed by the ILMI community named in the message.</li> <li>• <b>ASN parse errors</b>—Total number of ASN.1 or BER errors encountered by the ILMI entity when decoding received ILMI messages.</li> <li>• <b>Too bigs</b>—Total number of ILMI packets delivered to the ILMI entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names</b>—Total number of ILMI packets delivered to the ILMI entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values</b>—Total number of ILMI packets delivered to the ILMI entity with an error status field of <b>badValue</b>.</li> <li>• <b>Read onlys</b>—Total number of valid ILMI packets delivered to the ILMI entity with an error status field of <b>readOnly</b>. Only incorrect implementations of ILMI generate this error.</li> <li>• <b>General errors</b>—Total number of ILMI packets delivered to the ILMI entity with an error status field of <b>genErr</b>.</li> <li>• <b>Total request varbinds</b>—Total number of objects retrieved successfully by the ILMI entity as a result of receiving valid ILMI <b>GetRequest</b> and <b>GetNext</b> packets.</li> <li>• <b>Total set varbinds</b>—Total number of objects modified successfully by the ILMI entity as a result of receiving valid ILMI <b>SetRequest</b> packets.</li> <li>• <b>Get requests</b>—Total number of ILMI <b>GetRequest</b> packets that have been accepted and processed by the ILMI entity.</li> <li>• <b>Get nexts</b>—Total number of ILMI <b>GetNext</b> packets that have been accepted and processed by the ILMI entity.</li> <li>• <b>Set requests</b>—Total number of ILMI <b>SetRequest</b> packets that have been accepted and processed by the ILMI entity.</li> <li>• <b>Get responses</b>—Total number of ILMI <b>GetResponse</b> packets that have been accepted and processed by the ILMI entity.</li> <li>• <b>Traps</b>—Total number of ILMI traps received by the ILMI entity.</li> <li>• <b>Silent drops</b>—Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequest</b>, and <b>InformRequest</b> packets delivered to the ILMI entity that were silently dropped because the size of a reply containing an alternate response packet with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.</li> <li>• <b>Proxy drops</b>—Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequest</b>, and <b>InformRequest</b> packets delivered to the ILMI entity that were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in such a way (other than a timeout) that no response packet could be returned.</li> </ul> |
| <b>Output</b> | <p>Information about transmitted ILMI packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets</b>—Total number of messages passed from the ILMI entity to the transport service.</li> <li>• <b>Too bigs</b>—Total number of ILMI packets generated by the ILMI entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names</b>—Total number of ILMI packets generated by the ILMI entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values</b>—Total number of ILMI packets generated by the ILMI entity with an error status field of <b>badValue</b>.</li> <li>• <b>General errors</b>—Total number of ILMI packets generated by the ILMI entity with an error status field of <b>genErr</b>.</li> <li>• <b>Get requests</b>—Total number of ILMI <b>GetRequest</b> packets that have been generated by the ILMI entity.</li> <li>• <b>Get nexts</b>—Total number of ILMI <b>GetNext</b> packets that have been generated by the ILMI entity.</li> <li>• <b>Set requests</b>—Total number of ILMI <b>SetRequest</b> packets that have been generated by the ILMI entity.</li> <li>• <b>Get responses</b>—Total number of ILMI <b>GetResponse</b> packets that have been generated by the ILMI entity.</li> <li>• <b>Traps</b>—Total number of ILMI traps generated by the ILMI entity.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Sample Output

### show ilmi statistics

```
user@host> show ilmi statistics
ILMI statistics:
 Input:
 Packets: 0, Bad versions: 0, Bad community names: 0,
 Bad community uses: 0, ASN parse errors: 0,
 Too bigs: 0, No such names: 0, Bad values: 0,
 Read onlys: 0, General errors: 0,
 Total request varbinds: 0, Total set varbinds: 0,
 Get requests: 0, Get nexts: 0, Set requests: 0,
 Get responses: 0, Traps: 0,
 Silent drops: 0, Proxy drops 0
 Output:
 Packets: 0, Too bigs: 0, No such names: 0,
 Bad values: 0, General errors: 0,
 Get requests: 0, Get nexts: 0, Set requests: 0,
 Get responses: 0, Traps: 0
```

## show security alarms

---

**Syntax**    show security alarms  
              <detail>  
              <alarm-id *id-number*>  
              <alarm-type [ *types* ]>  
              <newer-than YYYY-MM-DD.HH:MM:SS>  
              <older-than YYYY-MM-DD.HH:MM:SS>  
              <process *process*>  
              <severity *severity*>

**Release Information**    Command introduced in Junos OS Release 11.2.

**Description**    Display the alarms that are active on the device. Run this command when the CLI prompt indicates that a security alarm has been raised, as shown here:

```
[1 SECURITY ALARM] user@host#
```

**Options**    **none**—Display all active alarms.

**detail**—(Optional) Display detailed output.

**alarm-id *id-number***—(Optional) Display the specified alarm.

**alarm-type [ *types* ]**—(Optional) Display the specified alarm type or a set of types.

You can specify one or more of the following alarm types:

- authentication
- cryptographic-self-test
- decryption-failures
- encryption-failures
- ike-phase1-failures
- ike-phase2-failures
- key-generation-self-test
- non-cryptographic-self-test
- policy
- replay-attacks

**newer-than YYYY-MM-DD.HH:MM:SS**—(Optional) Display active alarms that were raised after the specified date and time.

**older-than YYYY-MM-DD.HH:MM:SS**—(Optional) Display active alarms that were raised before the specified date and time.

**process *process***—(Optional) Display active alarms that were raised by the specified system process.

**severity severity**—(Optional) Display active alarms of the specified severity.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

**Required Privilege Level** security—To view this statement in the configuration.

**Related Documentation**

- [clear security alarms](#)
- [Example: Generating a Security Alarm in Response to Policy Violations](#)

**List of Sample Output**

[show security alarms on page 2176](#)  
[show security alarms detail on page 2176](#)  
[show security alarms alarm-id on page 2176](#)  
[show security alarms alarm-type authentication on page 2176](#)  
[show security alarms newer-than <time> on page 2177](#)  
[show security alarms older-than <time> on page 2177](#)  
[show security alarms process <process> on page 2177](#)  
[show security alarms severity <severity> on page 2177](#)

**Output Fields** [Table 241](#) lists the output fields for the **show security alarms** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the **detail** keyword is used.

**Table 241: show security alarms**

| Field Name        | Field Description                                                                                        | Level of Output |
|-------------------|----------------------------------------------------------------------------------------------------------|-----------------|
| <b>ID</b>         | Identification number of the alarm.                                                                      | All levels      |
| <b>Alarm time</b> | Date and time the alarm was raised..                                                                     | All levels      |
| <b>Message</b>    | Information about the alarm, including the alarm type, username, IP address, and port number.            | All levels      |
| <b>Process</b>    | System process (For example, login or sshd) and process identification number associated with the alarm. | <b>detail</b>   |

Table 241: show security alarms (*continued*)

| Field Name | Field Description            | Level of Output |
|------------|------------------------------|-----------------|
| Severity   | Severity level of the alarm. | detail          |

## Sample Output

### show security alarms

```
[3 SECURITY ALARMS] user@router> show security alarms
```

```

ID Alarm time Message
1 2010-01-19 13:41:36 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
failures (1) for user 'user' reached from '203.0.113.2'
2 2010-01-19 13:41:52 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
failures (1) for user 'user' reached from '203.0.113.2'
3 2010-01-19 13:42:13 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
failures (1) for user 'user' reached from '203.0.113.2'
```

### show security alarms detail

```
[3 SECURITY ALARMS] user@router> show security alarms detail
```

```

Alarm ID : 1
Alarm Type : authentication
Time : 2010-01-19 13:41:36 PST
Message : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2'
Process : sshd (pid 1414)
Severity : notice

Alarm ID : 2
Alarm Type : authentication
Time : 2010-01-19 13:41:52 PST
Message : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2'
Process : sshd (pid 1414)
Severity : notice

Alarm ID : 3
Alarm Type : authentication
Time : 2010-01-19 13:42:13 PST
Message : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
user 'user' reached from '203.0.113.2'
Process : sshd (pid 1414)
Severity : notice
```

### show security alarms alarm-id

```
[3 SECURITY ALARMS] user@router> show security alarms alarm-id 1
```

```

ID Alarm time Message
1 2010-01-19 13:41:36 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
failures (1) for user 'user' reached from '203.0.113.2'
```

### show security alarms alarm-type authentication

```
[3 SECURITY ALARMS] user@router> show security alarms alarm-type authentication
```



| ID | Alarm time              | Message                                                                                                    |
|----|-------------------------|------------------------------------------------------------------------------------------------------------|
| 1  | 2010-01-19 13:41:36 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 2  | 2010-01-19 13:41:52 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 3  | 2010-01-19 13:42:13 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |

#### show security alarms newer-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms newer-than 2010-01-19.13:41:59
```

|   |                         |                                                                                                            |
|---|-------------------------|------------------------------------------------------------------------------------------------------------|
| 3 | 2010-01-19 13:42:13 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
|---|-------------------------|------------------------------------------------------------------------------------------------------------|

#### show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms older-than 2010-01-19.13:41:59
```

| ID | Alarm time              | Message                                                                                                    |
|----|-------------------------|------------------------------------------------------------------------------------------------------------|
| 1  | 2010-01-19 13:41:36 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 2  | 2010-01-19 13:41:52 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |

#### show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> show security alarms process sshd
```

| ID | Alarm time              | Message                                                                                                    |
|----|-------------------------|------------------------------------------------------------------------------------------------------------|
| 1  | 2010-01-19 13:41:36 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 2  | 2010-01-19 13:41:52 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 3  | 2010-01-19 13:42:13 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |

#### show security alarms severity <severity>

```
[3 SECURITY ALARMS] user@router> show security alarms severity notice
```

| ID | Alarm time              | Message                                                                                                    |
|----|-------------------------|------------------------------------------------------------------------------------------------------------|
| 1  | 2010-01-19 13:41:36 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 2  | 2010-01-19 13:41:52 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |
| 3  | 2010-01-19 13:42:13 PST | SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '203.0.113.2' |

## show security datapath-debug capture

|                                 |                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security datapath-debug capture                                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.0.                                                                                                                                                           |
| <b>Description</b>              | Display details of the data path debugging capture file.                                                                                                                                               |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show security datapath-debug counter on page 2179</a></li> <li>• <a href="#">Understanding Data Path Debugging for Logical Systems</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security datapath—debug capture on page 2178</a>                                                                                                                                      |
| <b>Output Fields</b>            | Output fields are listed in the approximate order in which they appear.                                                                                                                                |

## Sample Output

### show security datapath—debug capture

```

user@host> show security datapath-debug capture
Packet 1, len 120: (C0/F0/P0/SEQ:71:1bt)
91 00 00 47 11 00 10 00 9a 14 00 19 03 00 00 00
00 00 00 00 00 01 00 47 10 00 00 00 00 00 00 00
00 1f 12 f8 dd 29 00 21 59 84 f4 01 81 00 02 1e
08 00 45 60 01 f4 00 00 00 00 3f 06 73 9f 01 01
01 02 03 01 01 02 d4 31 d4 31 00 00 00 00 00 00
00 00 50 02 00 00 ff ad 00 00 00 00
Packet 2, len 120: (C0/F0/P0/SEQ:71:1bt)
90 00 00 47 04 00 00 00 00 00 00 00 02 02 00 47
10 00 00 00 00 00 00 00 50 00 a6 1c 00 00 00 00
00 00 00 0a 00 00 00 00 00 00 09 d9 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 1f 12 f8
dd 29 00 21 59 84 f4 01 81 00 02 1e

```

## show security datapath-debug counter

|                                 |                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security datapath-debug counter                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.0.                                                                                                                                                  |
| <b>Description</b>              | Display details of the data path debugging counter.                                                                                                                                           |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show security datapath-debug capture on page 2178</a></li> <li>• <i>Understanding Data Path Debugging for Logical Systems</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security datapath-debug counter on page 2179</a>                                                                                                                             |
| <b>Output Fields</b>            | Output fields are listed in the approximate order in which they appear.                                                                                                                       |

### Sample Output

#### show security datapath-debug counter

```

user@host> show security datapath-debug counter
Datapath debug counters
Packet Filter 1:
np-ingress
Chassis 0 FPC 4 : 1
np-ingress
Chassis 0 FPC 3 : 0
np-egress
Chassis 0 FPC 4 : 1
np-egress
Chassis 0 FPC 3 : 0
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 2
pot
Chassis 0 FPC 0 PIC 1: 0
pot

```

## show security monitoring

|                                 |                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security monitoring                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.2.                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Displays a count of security flow and central point (CP) sessions, CPU utilization (as a percentage of maximum), and memory in use (also as a percentage of maximum) at the moment the command is run.                                                                                         |
| <b>Required Privilege Level</b> | View                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show security monitoring fpc fpc-number on page 2182</a></li> <li>• <a href="#">show security monitoring performance session on page 2185</a></li> <li>• <a href="#">show security monitoring performance spu on page 2186</a></li> </ul> |

## show security monitoring

```
user@host>show security monitoring
```

```
user@host> show security monitoring
```

| FPC   | PIC       | CPU | Mem | Flow session<br>current | Flow session<br>maximum | CP session<br>current | CP session<br>maximum |
|-------|-----------|-----|-----|-------------------------|-------------------------|-----------------------|-----------------------|
| 1     | 0         | 0   | 11  | 0                       | 0                       | 0                     | 0                     |
| 1     | 1         | 0   | 5   | 3                       | 6291456                 | 1                     | 7549747               |
| 1     | 2         | 0   | 5   | 2                       | 6291456                 | 0                     | 7549747               |
| 1     | 3         | 0   | 5   | 3                       | 6291456                 | 1                     | 7549747               |
| 8     | 0         | 0   | 65  | 4                       | 6963                    | 2                     | 8355                  |
| 8     | 1         | 0   | 65  | 2                       | 6963                    | 0                     | 8355                  |
| Total | Sessions: |     |     | 14                      | 18888294                | 4                     | 22665951              |

## show security monitoring (vSRX)

```
user@host>show security monitoring
```

```
user@host> show security monitoring
```

| FPC | PIC | CPU | Mem | Flow session<br>current | Flow session<br>maximum | CP session<br>current | CP session<br>maximum |
|-----|-----|-----|-----|-------------------------|-------------------------|-----------------------|-----------------------|
| 0   | 0   | 0   | 68  | 2                       | 524288                  | N/A                   | N/A                   |

## show security monitoring (vSRX in a Chassis Cluster)

```
user@host>show security monitoring
```

```
node0:
```

| FPC | PIC | CPU | Mem | Flow session<br>current | Flow session<br>maximum | CP session<br>current | CP session<br>maximum |
|-----|-----|-----|-----|-------------------------|-------------------------|-----------------------|-----------------------|
|-----|-----|-----|-----|-------------------------|-------------------------|-----------------------|-----------------------|

|   |   |   |    |   |        |     |     |
|---|---|---|----|---|--------|-----|-----|
| 0 | 0 | 0 | 67 | 0 | 524288 | N/A | N/A |
|---|---|---|----|---|--------|-----|-----|

node1:

| FPC | PIC | CPU | Mem | Flow session<br>current | Flow session<br>maximum | CP session<br>current | CP session<br>maximum |
|-----|-----|-----|-----|-------------------------|-------------------------|-----------------------|-----------------------|
| 0   | 0   | 0   | 67  | 0                       | 524288                  | N/A                   | N/A                   |

## show security monitoring fpc fpc-number

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show security monitoring fpc <i>fpc-number</i></b><br><node ( <i>node-id</i>   all   local   primary )>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display security monitoring information about the FPC slot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b><i>fpc-number</i></b>—Display security monitoring information for the specified FPC slot. It can be in the range from 0 to 11.</li> <li>• <b>node</b>—(Optional) For chassis cluster configurations, display security monitoring information for the specified FPC on a specific node (device) in the cluster. <ul style="list-style-type: none"> <li>• <b><i>node-id</i></b>—Identification number of the node. It can be 0 or 1.</li> <li>• <b>all</b>—Display information about all nodes.</li> <li>• <b>local</b>—Display information about the local node.</li> <li>• <b>primary</b>—Display information about the primary node.</li> </ul> </li> </ul> |
| <b>Additional Information</b>   | For complete list of slot numbering, physical port, and logical interface numbering for SRX Series devices in chassis cluster, see <i>Chassis Cluster Feature Guide for Branch SRX Series Devices</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show services ip-monitoring status on page 2187</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show security monitoring fpc 0 on page 2183</a><br><a href="#">show security monitoring fpc 1 on page 2183</a><br><a href="#">show security monitoring fpc 8 on page 2184</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Output Fields</b>            | <a href="#">Table 242</a> lists the output fields for the <b>show security monitoring fpc <i>fpc-number</i></b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 242: show security monitoring fpc fpc-number Output Fields**

| Field Name             | Field Description                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPC                    | Slot number in which the FPC is installed.                                                                                                                       |
| PIC                    | Slot number in which the PIC is installed.                                                                                                                       |
| CPU Utilization (%)    | Total percentage of CPU being used by the PIC's processors.                                                                                                      |
| Memory Utilization (%) | Percentage of heap space (dynamic memory) being used by the PIC's processor. If this number exceeds 80 percent, there might be a software problem (memory leak). |

Table 242: show security monitoring fpc fpc-number Output Fields (*continued*)

| Field Name                    | Field Description                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Current flow session</b>   | The current number of flow sessions. When SRX Series devices operate in packet mode, flow sessions will not be created and this field will remain zero. |
| <b>Max flow session</b>       | The maximum number of flow sessions allowed. This number will differ from one device to another.                                                        |
| <b>SPU current cp session</b> | The current number of cp sessions for the SPU (on SRX5600, and SRX5800 devices only).                                                                   |
| <b>SPU max cp session</b>     | The maximum number of cp sessions allowed for the SPU (on SRX5600, and SRX5800 devices only).                                                           |

## Sample Output

### show security monitoring fpc 0

```

user@host> show security monitoring fpc 0
FPC 0
 PIC 0
 CPU utilization : 0 %
 Memory utilization : 82 %
 Current flow session : 0
 Max flow session : 0
 Current CP session : 0
 Max CP session : 12000000
 Session Creation Per Second (for last 96 seconds on average): 0
 PIC 1
 CPU utilization : 0 %
 Memory utilization : 54 %
 Current flow session : 0
 Max flow session : 819200
 Current CP session : 0
 Max CP session : 0
 Session Creation Per Second (for last 96 seconds on average): 0

```

## Sample Output

### show security monitoring fpc 1

```

user@host> show security monitoring fpc 1
FPC 1
 PIC 0
 CPU utilization : 0 %
 Memory utilization : 21 %
 Current flow session : 0
 Max flow session : 524288
 Current CP session : 0
 Max CP session : 1048576
 Session Creation Per Second (for last 96 seconds on average): 0

```

## Sample Output

### show security monitoring fpc 8

```
user@host> show security monitoring fpc 5
FPC 5
 PIC 0
 CPU utilization : 0 %
 Memory utilization : 64 %
 Current flow session : 0
 Max flow session : 524288
 Current CP session : 0
 Max CP session : 2359296
 Session Creation Per Second (for last 96 seconds on average): 0
 PIC 1
 CPU utilization : 0 %
 Memory utilization : 65 %
 Current flow session : 0
 Max flow session : 1048576
 Current CP session : 0
 Max CP session : 0
 Session Creation Per Second (for last 96 seconds on average): 0
```



## show security monitoring performance session

**Syntax** show security monitoring performance session

<fpc slot-number>

<pic slot-number>

**Release Information** Command introduced in Junos OS Release of 10.2.

**Description** Display the current session (total number of sessions at that time) for the last 60 seconds.

- Options**
- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
  - **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.



**NOTE:** The `fpc slot-number` and `pic slot-number` options are not available on SRX300, SRX320, and SRX340 devices.

**Required Privilege Level** View

**Related Documentation**

- [show services ip-monitoring status on page 2187](#)

## show security monitoring performance session

```
user@host> show security monitoring performance session
```

```
fpc 0 pic 0
Last 60 seconds:
0: 8 1: 8 2: 8 3: 8 4: 8 5: 7
6: 7 7: 7 8: 7 9: 7 10: 7 11: 8
12: 8 13: 8 14: 7 15: 7 16: 7 17: 7
18: 7 19: 7 20: 7 21: 5 22: 5 23: 5
24: 5 25: 5 26: 5 27: 5 28: 5 29: 4
30: 4 31: 4 32: 3 33: 3 34: 3 35: 3
36: 5 37: 5 38: 6 39: 6 40: 5 41: 5
42: 5 43: 5 44: 5 45: 5 46: 5 47: 5
48: 7 49: 7 50: 6 51: 8 52: 8 53: 6
54: 5 55: 7 56: 7 57: 5 58: 5 59: 8
```

## show security monitoring performance spu

**Syntax** show security monitoring performance spu

<fpc slot-number>

<pic slot-number>

**Release Information** Command introduced in Junos OS Release 10.2.

**Description** Display the services processing unit (SPU) percent utilization for all FPC slots over the last 60 seconds. Use this command to track the percent utilization statistics per second for the past 60 seconds for each FPC slot and PIC.

- Options**
- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
  - **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.



**NOTE:** The **fpc slot-number** and **pic slot-number** options are not available on SRX300, SRX320, or SRX340 devices or on vSRX instances.

**Required Privilege Level** View

**Related Documentation**

- [show services ip-monitoring status on page 2187](#)

## show security monitoring performance spu

This sample shows 46% utilization of the SPU for second 42 in the past 60 seconds for FPC 0 and PIC 0.

user@host>show security monitoring performance spu

```
fpc 0 pic 0
Last 60 seconds:
0: 48 1: 48 2: 48 3: 48 4: 48 5: 48
6: 48 7: 48 8: 49 9: 48 10: 48 11: 48
12: 48 13: 48 14: 48 15: 48 16: 48 17: 48
18: 48 19: 48 20: 48 21: 48 22: 49 23: 48
24: 49 25: 49 26: 48 27: 48 28: 48 29: 48
30: 48 31: 48 32: 48 33: 48 34: 48 35: 48
36: 46 37: 47 38: 46 39: 46 40: 46 41: 46
42: 46 43: 46 44: 46 45: 46 46: 46 47: 46
48: 46 49: 46 50: 46 51: 46 52: 46 53: 46
54: 46 55: 46 56: 46 57: 46 58: 46 59: 46
```

## show services ip-monitoring status

|                                 |                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services ip-monitoring status                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command modified in Junos OS Release 11.4 R2. Next-hop functionality added in Junos OS Release 12.1X46-D15.                                                                                                                                                                                                                                 |
| <b>Description</b>              | Display a brief summary of IP monitoring status along with the current state for a given policy.                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show services rpm probe-results (View)</a></li> </ul>                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">show services ip-monitoring status on page 2188</a><br><a href="#">show services ip-monitoring status on page 2188</a><br><a href="#">show services ip-monitoring status on page 2189</a><br><a href="#">show services ip-monitoring status on page 2189</a><br><a href="#">show services ip-monitoring status on page 2189</a> |
| <b>Output Fields</b>            | Table 243 lists the output fields for the <b>show services ip-monitoring status</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                        |

Table 243: show services ip-monitoring status Output Fields

| Field Name              | Field Description                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy</b>           | Name of the policy configured.                                                                                                |
| <b>Probe Name</b>       | Name of the probe configured.                                                                                                 |
| <b>Address</b>          | Displays the configured target address.                                                                                       |
| <b>Status</b>           | Displays the status of the probe on the target address. If the status is PASS, then the target address is reached.            |
| <b>Route-Action</b>     | Displays route injection information configured for the policy and its failover status.                                       |
| <b>Route-Instance</b>   | Displays the routing instance of the route to be injected during failover.                                                    |
| <b>Route</b>            | Routing address of the route to be injected during failover.                                                                  |
| <b>Next-Hop</b>         | Specifies the next-hop address of the route to be injected during failover. P2P interfaces only.                              |
| <b>State</b>            | Display the state of the route injection action. If the state is APPLIED, then the ip-monitoring policy is in failover state. |
| <b>Interface Action</b> | Displays the interface action type as enable or disable.                                                                      |

Table 243: show services ip-monitoring status Output Fields (*continued*)

| Field Name    | Field Description                                     |
|---------------|-------------------------------------------------------|
| Policy Action | Displays the policy action type as enable or disable. |
| Admin State   | Displays the current admin state of the interface.    |
| Action Status | Displays the current action status of the interface.  |

## Sample Output

### show services ip-monitoring status

```

user@host> show services ip-monitoring status

Policy - policy1 (Non-preemptive. Status: FAIL)
RPM Probes:
 Probe name Test Name Address Status

 probe_a a1 15.1.1.10 FAIL
 probe_a a2 200.1.1.1 FAIL
Route-Action:
 route-instance route next-hop State

 inet.0 200.1.1.0 150.1.1.1 APPLIED
Interface-Action:
 interface policy action admin state action status

 fe-0/0/5.2 Enable UP FAILOVER
 fe-0/0/5.4 Disable DOWN FAILOVER
 t1-1/0/0 Enable UP FAILOVER
 d10 Enable UP FAILOVER
 ge-0/0/1 Enable UP FAILOVER

```

## Sample Output

### show services ip-monitoring status

In this example, the policy is in the failback state, and the no-preempt option is not configured.

```

user@host> show services ip-monitoring status

Policy - policy1 (Status: PASS)
RPM Probes:
 Probe name Test Name Address Status

 probe1 a1 99.1.1.2 PASS
Route-Action:
 route-instance route next-hop state

 inet.0 99.1.1.0 12.12.12.2 NOT-APPLIED
Interface-Action:
 interface policy action admin state action status

```

|            |        |      |             |
|------------|--------|------|-------------|
| at-2/0/0   | Enable | DOWN | MARKED-DOWN |
| ge-0/0/2.2 | Enable | DOWN | MARKED-DOWN |
| ge-0/0/2.3 | Enable | DOWN | MARKED-DOWN |

## Sample Output

### show services ip-monitoring status

In this example, the policy is in the failover state, and the primary is restored. The no-preempt option is configured.

```
user@host> show services ip-monitoring status
```

Policy - policy1 (Non-preemptive. Status: FAILOVER-NO-PREEMPT)

RPM Probes:

| Probe name | Test Name | Address  | Status |
|------------|-----------|----------|--------|
| probe1     | a1        | 99.1.1.2 | PASS   |

Route-Action:

| route-instance | route    | next-hop   | state   |
|----------------|----------|------------|---------|
| inet.0         | 99.1.1.0 | 12.12.12.2 | APPLIED |

Interface-Action:

| interface  | policy action | admin state | action status |
|------------|---------------|-------------|---------------|
| at-2/0/0   | Enable        | UP          | FAILOVER      |
| ge-0/0/2.2 | Enable        | UP          | FAILOVER      |
| ge-0/0/2.3 | Enable        | UP          | FAILOVER      |

## Sample Output

### show services ip-monitoring status

When the probe succeeds and the policy is not applied, the output is as follows:

```
user@host> show services ip-monitoring status
```

Policy payment (Status: PASS)

RPM Probes:

| Probe name           | Test Name | Address | Status |
|----------------------|-----------|---------|--------|
| Probe-Payment-Server | paysvr    | 9.9.9.2 | PASS   |

Route-Action:

| route-instance | route      | next-hop   | state       |
|----------------|------------|------------|-------------|
| inet.0         | 9.9.9.0/24 | e1-6/0/0.0 | NOT-APPLIED |

## Sample Output

### show services ip-monitoring status

When the probe fails and the policy is applied, the output is as follows:

```
user@host> show services ip-monitoring status
```

Policy payment (Status: FAIL)

RPM Probes:

| Probe name           | Test Name | Address | Status |
|----------------------|-----------|---------|--------|
| Probe-Payment-Server | paysvr    | 9.9.9.2 | FAIL   |

Route-Action:

| route-instance | route | next-hop | state |
|----------------|-------|----------|-------|
|----------------|-------|----------|-------|

|        |            |            |         |
|--------|------------|------------|---------|
| -----  | -----      | -----      | -----   |
| inet.0 | 9.9.9.0/24 | e1-6/0/0.0 | APPLIED |

## show snmp health-monitor

|                                 |                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show snmp health-monitor</code><br><code>&lt;alarms &lt;detail&gt;&gt;   &lt;logs&gt;</code>                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.0.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                             |
| <b>Description</b>              | Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.                                                                                                                                                                |
| <b>Options</b>                  | <b>none</b> —Display information about all health monitor alarms and logs.<br><br><b>alarms &lt;detail&gt;</b> —(Optional) Display detailed information about health monitor alarms.<br><br><b>logs</b> —(Optional) Display information about health monitor logs. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show snmp health-monitor on page 2193</a><br><a href="#">show snmp health-monitor alarms detail on page 2195</a>                                                                                                                                       |
| <b>Output Fields</b>            | <a href="#">Table 244</a> describes the output fields for the <b>show snmp health-monitor</b> command. Output fields are listed in the approximate order in which they appear.                                                                                     |

**Table 244: show snmp health-monitor Output Fields**

| Field Name                  | Field Description                                                           | Level of Output |
|-----------------------------|-----------------------------------------------------------------------------|-----------------|
| <b>Alarm Index</b>          | Alarm identifier.                                                           | All levels      |
| <b>Variable description</b> | Description of the health monitor object instance being monitored.          | All levels      |
| <b>Variable name</b>        | Name of the health monitor object instance being monitored.                 | All levels      |
| <b>Value</b>                | Current value of the monitored variable in the most recent sample interval. | All levels      |

Table 244: show snmp health-monitor Output Fields (*continued*)

| Field Name              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Level of Output |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>State</b>            | <p>State of the alarm or event entry:</p> <ul style="list-style-type: none"> <li>Alarms: <ul style="list-style-type: none"> <li><b>active</b>—Entry is fully configured and activated.</li> <li><b>falling threshold crossed</b>—Value of the variable has crossed the lower threshold limit.</li> <li><b>rising threshold crossed</b>—Value of the variable has crossed the upper threshold limit.</li> <li><b>under creation</b>—Entry is being configured and is not yet activated.</li> <li><b>startup</b>—Alarm is waiting for the first sample of the monitored variable.</li> <li><b>object not available</b>—Monitored variable of that type is not available to the health monitor agent.</li> <li><b>instance not available</b>—Monitored variable's instance is not available to the health monitor agent.</li> <li><b>object type invalid</b>—Monitored variable is not a numeric value.</li> <li><b>object processing errored</b>—An error occurred when the monitored variable was processed.</li> <li><b>unknown</b>—State is not one of the above.</li> </ul> </li> </ul> | All levels      |
| <b>Variable OID</b>     | Object ID to which the variable name is resolved. The format is x.x.x.x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | detail          |
| <b>Sample type</b>      | Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of <b>absolute value</b> or <b>delta value</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | detail          |
| <b>Startup alarm</b>    | <p>Alarm that might be sent when this entry is first activated, depending on the following criteria:</p> <ul style="list-style-type: none"> <li>Alarm is sent when one of the following situations exists: <ul style="list-style-type: none"> <li>Value of the alarm is above or equal to the rising threshold and the startup type is either <b>rising alarm</b> or <b>rising or falling alarm</b>.</li> <li>Value of the alarm is below or equal to the falling threshold and the startup type is either <b>falling alarm</b> or <b>rising or falling alarm</b>.</li> </ul> </li> <li>Alarm is <i>not</i> sent when one of the following situations exists: <ul style="list-style-type: none"> <li>Value of the alarm is above or equal to the rising threshold and the startup type is <b>falling alarm</b>.</li> <li>Value of the alarm is below or equal to the falling threshold and the startup type is <b>rising alarm</b>.</li> <li>Value of the alarm is between the thresholds.</li> </ul> </li> </ul>                                                                         | detail          |
| <b>Owner</b>            | Name of the entry configured by the user. If the entry was created through the CLI, the owner has <b>monitor</b> prepended to it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | detail          |
| <b>Creator</b>          | Mechanism by which the entry was configured ( <b>Health Monitor</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | detail          |
| <b>Sample interval</b>  | Time period between samples (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | detail          |
| <b>Rising threshold</b> | Upper limit threshold value as a percentage of the maximum possible value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | detail          |



Table 244: show snmp health-monitor Output Fields (*continued*)

| Field Name          | Field Description                                                          | Level of Output |
|---------------------|----------------------------------------------------------------------------|-----------------|
| Falling threshold   | Lower limit threshold value as a percentage of the maximum possible value. | detail          |
| Rising event index  | Event triggered when the rising threshold is crossed.                      | detail          |
| Falling event index | Event triggered when the falling threshold is crossed.                     | detail          |

## Sample Output

### show snmp health-monitor

```
user@host> show snmp health-monitor
```

```

Alarm
Index Variable description Value State

32768 Health Monitor: root file system utilization
 jnxHrStoragePercentUsed.1 58 active

32769 Health Monitor: /config file system utilization
 jnxHrStoragePercentUsed.2 0 active

32770 Health Monitor: RE 0 CPU utilization
 jnxOperatingCPU.9.1.0.0 0 active

32773 Health Monitor: RE 0 Memory utilization
 jnxOperatingBuffer.9.1.0.0 35 active

32775 Health Monitor: jkernel daemon CPU utilization
 Init daemon 0 active
 Chassis daemon 50 active
 Firewall daemon 0 active
 Interface daemon 5 active
 SNMP daemon 11 active
 MIB2 daemon 42 active
 Sonet APS daemon 0 active
 VRRP daemon 0 active
 Alarm daemon 3 active
 PFE daemon 0 active
 CRAFT daemon 0 active
 Traffic sampling control daemon 0 active
 Ilmi daemon 0 active
 Remote operations daemon 0 active
 CoS daemon 0 active
 Pic Services Logging daemon 0 active
 Internal Routing Service Daemon 3 active
 Network Access Service daemon 0 active
 Forwarding UDP daemon 0 active
 Routing socket proxy daemon 0 active
 Disk Monitoring daemon 1 active
 Inet daemon 0 active
 Syslog daemon 0 active
 Adaptive Services PIC daemon 0 active
 ECC parity errors logging Daemon 0 active
 Layer 2 Tunneling Protocol daemon 0 active
 PPPoE daemon 3 active

```

|       |                                                   |              |
|-------|---------------------------------------------------|--------------|
|       | Redundancy device daemon                          | 0 active     |
|       | PPP daemon                                        | 0 active     |
|       | Dynamic Flow Capture Daemon                       | 0 active     |
| 32776 | Health Monitor: jroute daemon CPU utilization     |              |
|       | Routing protocol daemon                           | 1 active     |
|       | Management daemon                                 | 0 active     |
|       | Management daemon                                 | 0 active     |
|       | Command line interface                            | 4 active     |
|       | Periodic Packet Management daemon                 | 0 active     |
|       | Link Management daemon                            | 0 active     |
|       | Pragmatic General Multicast daemon                | 0 active     |
|       | Bidirectional Forwarding Detection daemon         | 0 active     |
|       | SRC daemon                                        | 0 active     |
|       | audit daemon                                      | 0 active     |
|       | Event daemon                                      | 0 active     |
| 32777 | Health Monitor: jcrypto daemon CPU utilization    |              |
|       | IPSec Key Management daemon                       | 0 active     |
| 32779 | Health Monitor: jkernel daemon Memory utilization |              |
|       | Init daemon                                       | 47384 active |
|       | Chassis daemon                                    | 20204 active |
|       | Firewall daemon                                   | 1956 active  |
|       | Interface daemon                                  | 3340 active  |
|       | SNMP daemon                                       | 4540 active  |
|       | MIB2 daemon                                       | 3880 active  |
|       | Sonet APS daemon                                  | 2632 active  |
|       | VRRP daemon                                       | 2672 active  |
|       | Alarm daemon                                      | 1856 active  |
|       | PFE daemon                                        | 2600 active  |
|       | CRAFT daemon                                      | 2000 active  |
|       | Traffic sampling control daemon                   | 3164 active  |
|       | Ilmi daemon                                       | 2132 active  |
|       | Remote operations daemon                          | 2964 active  |
|       | CoS daemon                                        | 3044 active  |
|       | Pic Services Logging daemon                       | 1944 active  |
|       | Internal Routing Service Daemon                   | 1392 active  |
|       | Network Access Service daemon                     | 1992 active  |
|       | Forwarding UDP daemon                             | 1876 active  |
|       | Routing socket proxy daemon                       | 1296 active  |
|       | Disk Monitoring daemon                            | 1180 active  |
|       | Inet daemon                                       | 1296 active  |
|       | Syslog daemon                                     | 1180 active  |
|       | Adaptive Services PIC daemon                      | 3220 active  |
|       | ECC parity errors logging Daemon                  | 1100 active  |
|       | Layer 2 Tunneling Protocol daemon                 | 3372 active  |
|       | PPPoE daemon                                      | 1424 active  |
|       | Redundancy device daemon                          | 1820 active  |
|       | PPP daemon                                        | 2060 active  |
|       | Dynamic Flow Capture Daemon                       | 10740 active |
| 32780 | Health Monitor: jroute daemon Memory utilization  |              |
|       | Routing protocol daemon                           | 8104 active  |
|       | Management daemon                                 | 13360 active |
|       | Management daemon                                 | 19252 active |
|       | Command line interface                            | 9912 active  |
|       | Periodic Packet Management daemon                 | 1484 active  |
|       | Link Management daemon                            | 2016 active  |
|       | Pragmatic General Multicast daemon                | 1968 active  |
|       | Bidirectional Forwarding Detection daemon         | 1956 active  |
|       | SRC daemon                                        | 1772 active  |

```

audit daemon 1772 active
Event daemon 1808 active

```

```

32781 Health Monitor: jcrypto daemon Memory utilization
IPSec Key Management daemon 5600 active

```

### show snmp health-monitor alarms detail

```
user@host> show snmp health-monitor alarms detail
```

```

Alarm Index 32768:
Variable name jnxHrStoragePercentUsed.1
Variable OID 1.3.6.1.4.1.2636.3.31.1.1.1.1.1
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: root file system
 utilization
Creator Health Monitor
State active
Sample interval 300 seconds
Rising threshold 80
Falling threshold 70
Rising event index 32768
Falling event index 32768
Instance Value: 58
Instance State: active

Alarm Index 32769:
Variable name jnxHrStoragePercentUsed.2
Variable OID 1.3.6.1.4.1.2636.3.31.1.1.1.1.2
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: /config file system
 utilization
Creator Health Monitor
State active
Sample interval 300 seconds
Rising threshold 80
Falling threshold 70
Rising event index 32768
Falling event index 32768
Instance Value: 0
Instance State: active

Alarm Index 32770:
Variable name jnxOperatingCPU.9.1.0.0
Variable OID 1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: RE 0 CPU utilization

Creator Health Monitor
State active
Sample interval 300 seconds
Rising threshold 80
Falling threshold 70
Rising event index 32768
Falling event index 32768
Instance Value: 0
Instance State: active

```

## Alarm Index 32773:

|               |                                         |
|---------------|-----------------------------------------|
| Variable name | jnxOperatingBuffer.9.1.0.0              |
| Variable OID  | 1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0    |
| Sample type   | absolute value                          |
| Startup alarm | rising alarm                            |
| Owner         | Health Monitor: RE 0 Memory utilization |

|                     |                |
|---------------------|----------------|
| Creator             | Health Monitor |
| State               | active         |
| Sample interval     | 300 seconds    |
| Rising threshold    | 80             |
| Falling threshold   | 70             |
| Rising event index  | 32768          |
| Falling event index | 32768          |
| Instance Value:     | 35             |
| Instance State:     | active         |

## Alarm Index 32775:

|               |                                                |
|---------------|------------------------------------------------|
| Variable name | sysAppElmtRunCPU.3                             |
| Variable OID  | 1.3.6.1.2.1.54.1.2.3.1.9.3                     |
| Sample type   | delta value                                    |
| Startup alarm | rising alarm                                   |
| Owner         | Health Monitor: jkernel daemon CPU utilization |

|                       |                        |
|-----------------------|------------------------|
| Creator               | Health Monitor         |
| State                 | active                 |
| Sample interval       | 300 seconds            |
| Rising threshold      | 24000                  |
| Falling threshold     | 21000                  |
| Rising event index    | 32768                  |
| Falling event index   | 32768                  |
| Instance Name:        | sysAppElmtRunCPU.3.1.1 |
| Instance Description: | Init daemon            |
| Instance Value:       | 0                      |
| Instance State:       | active                 |

|                       |                           |
|-----------------------|---------------------------|
| Instance Name:        | sysAppElmtRunCPU.3.2.2786 |
| Instance Description: | Chassis daemon            |
| Instance Value:       | 50                        |
| Instance State:       | active                    |

|                       |                           |
|-----------------------|---------------------------|
| Instance Name:        | sysAppElmtRunCPU.3.3.2938 |
| Instance Description: | Firewall daemon           |
| Instance Value:       | 0                         |
| Instance State:       | active                    |

|                       |                           |
|-----------------------|---------------------------|
| Instance Name:        | sysAppElmtRunCPU.3.4.2942 |
| Instance Description: | Interface daemon          |
| Instance Value:       | 5                         |
| Instance State:       | active                    |

|                       |                           |
|-----------------------|---------------------------|
| Instance Name:        | sysAppElmtRunCPU.3.7.7332 |
| Instance Description: | SNMP daemon               |
| Instance Value:       | 11                        |
| Instance State:       | active                    |

|                       |                           |
|-----------------------|---------------------------|
| Instance Name:        | sysAppElmtRunCPU.3.9.2914 |
| Instance Description: | MIB2 daemon               |
| Instance Value:       | 42                        |

```
Instance State: active

Instance Name: sysAppElemRunCPU.3.12.2916
Instance Description: Sonet APS daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.13.2917
Instance Description: VRRP daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.14.2787
Instance Description: Alarm daemon
Instance Value: 3
Instance State: active

Instance Name: sysAppElemRunCPU.3.15.2940
Instance Description: PFE daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.16.2788
Instance Description: CRAFT daemon
Instance Value: 0
Instance State: active

Instance Name: sysAppElemRunCPU.3.17.2918
Instance Description: Traffic sampling control daemon
---(more 23%)---
```

## show snmp inform-statistics

|                                 |                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show snmp inform-statistics                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| <b>Description</b>              | Display information about Simple Network Management Protocol (SNMP) inform requests.                                                                                                                                                                                              |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">show snmp inform-statistics on page 2198</a>                                                                                                                                                                                                                          |
| <b>Output Fields</b>            | <p><a href="#">Table 245</a> describes the output fields for the <b>show snmp inform-statistics</b> command.</p> <p>Output fields are listed in the approximate order in which they appear.</p>                                                                                   |

**Table 245: show snmp inform-statistics Output Fields**

| Field Name            | Field Description                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target Name</b>    | Name of the device configured to receive and respond to SNMP informs.                                                                              |
| <b>Address</b>        | IP address of the target device.                                                                                                                   |
| <b>Sent</b>           | Number of informs sent to the target device and acknowledged by the target device.                                                                 |
| <b>Pending</b>        | Number of informs held in memory pending a response from the target device.                                                                        |
| <b>Discarded</b>      | Number of informs discarded after the specified number of retransmissions to the target device were attempted.                                     |
| <b>Timeouts</b>       | Number of informs that did not receive an acknowledgement from the target device within the timeout specified.                                     |
| <b>Probe Failures</b> | Connection failures that occurred (for example, when the target server returned invalid content or you incorrectly configured the target address). |

## Sample Output

### show snmp inform-statistics

```

user@host> show snmp inform-statistics
Inform Request Statistics:
Target Name: TA1_v3_md5_none Address: 172.17.20.184
Sent: 176, Pending: 0
Discarded: 0, Timeouts: 0, Probe Failures: 0

```

Target Name: TA2\_v3\_sha\_none Address: 192.168.110.59  
Sent: 0, Pending: 4  
Discarded: 84, Timeouts: 0, Probe Failures: 258  
Target Name: TA5\_v2\_none Address: 172.17.20.184  
Sent: 0, Pending: 0  
Discarded: 2, Timeouts: 10, Probe Failures: 0

## show snmp mib

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show snmp mib (get   get-next   walk) (ascii   decimal) <i>object-id</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p><b>ascii</b> and <b>decimal</b> options introduced in Junos OS Release 9.6.</p> <p><b>ascii</b> and <b>decimal</b> options introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>get</b>—Retrieve and display one or more SNMP object values.</p> <p><b>get-next</b>—Retrieve and display the next SNMP object values.</p> <p><b>walk</b>—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.</p> <p><b>ascii</b>—Display the SNMP object's string indices as an ASCII-key representation.</p> <p><b>decimal</b>—Display the SNMP object values in the decimal (default) format. The <b>decimal</b> option is the default option for this command. Therefore, issuing the <b>show snmp mib (get   get-next   walk) decimal object-id</b> and the <b>show snmp mib (get   get-next   walk) object-id</b> commands display the same output.</p> <p><b>object-id</b>—The object can be represented by a sequence of dotted integers (such as 1.3.6.1.2.1.2) or by its subtree name (such as <b>interfaces</b>). When entering multiple objects, enclose the objects in quotation marks.</p> |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <p><a href="#">show snmp mib get on page 2201</a></p> <p><a href="#">show snmp mib get (Multiple Objects) on page 2201</a></p> <p><a href="#">show snmp mib get (Layer 2 Policer) on page 2201</a></p> <p><a href="#">show snmp mib get-next on page 2201</a></p> <p><a href="#">show snmp mib get-next (Specify an OID) on page 2201</a></p> <p><a href="#">show snmp mib walk on page 2201</a></p> <p><a href="#">show snmp mib walk (QFX Series) on page 2201</a></p> <p><a href="#">show snmp mib walk decimal on page 2202</a></p> <p><a href="#">show snmp mib walk (ASCII) on page 2202</a></p> <p><a href="#">show snmp mib walk (Multiple Indices) on page 2202</a></p> <p><a href="#">show snmp mib walk decimal (Multiple Indices) on page 2202</a></p>                                                                                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | Table 246 describes the output fields for the <b>show snmp mib</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



Table 246: show snmp mib Output Fields

| Field Name          | Field Description                                                               |
|---------------------|---------------------------------------------------------------------------------|
| <i>name</i>         | Object name and numeric instance value.                                         |
| <i>object value</i> | Object value. The Junos OS translates OIDs into the corresponding object names. |

## Sample Output

### show snmp mib get

```
user@host> show snmp mib get sysObjectID.0
sysObjectID.0 = jnxProductNameM20
```

### show snmp mib get (Multiple Objects)

```
user@host> show snmp mib get ?sysObjectID.0 sysUpTime.0?
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

### show snmp mib get (Layer 2 Policer)

```
user@host> show snmp mib get ifInOctets.25970
ifInOctets.25970 = 7545720
```

### show snmp mib get-next

```
user@host> show snmp mib get-next jnxMibs
jnxBoxClass.0 = jnxProductLineM20.0
```

### show snmp mib get-next (Specify an OID)

```
user@host> show snmp mib get-next 1.3.6.1
sysDescr.0 = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper
Networks, Inc.
```

### show snmp mib walk

```
user@host> show snmp mib walk system
sysDescr.0 = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004
Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
sysContact.0 = Your contact
sysName.0 = my router
sysLocation.0 = building 1
sysServices.0 = 4
```

### show snmp mib walk (QFX Series)

```
user@switch> show snmp mib walk system
sysDescr.0 = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0 = 138980301
sysContact.0 = System Contact
```

```
sysName.0 = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

#### show snmp mib walk decimal

```
user@host show snmp mib walk decimal jnxUtilData
jnxUtilCounter32Value.102.114.101.100 = 100
```

#### show snmp mib walk (ASCII)

```
show snmp mib walk ascii jnxUtilData
jnxUtilCounter32Value."fred" = 100
```

#### show snmp mib walk (Multiple Indices)

```
show snmp mib walk ascii jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.....
```

#### show snmp mib walk decimal (Multiple Indices)

```
show snmp mib walk decimal jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.....
```

## show snmp rmon

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show snmp rmon<br><alarms <brief   detail>   events <brief   detail>   logs>                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms and events.                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b>none</b>—Display information about all RMON alarms and events.</p> <p><b>alarms</b>—(Optional) Display information about RMON alarms.</p> <p><b>brief   detail</b>—(Optional) Display brief or detailed information about RMON alarms or events.</p> <p><b>events</b>—(Optional) Display information about RMON events.</p> <p><b>logs</b>—(Optional) Display information about RMON monitoring logs.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show snmp rmon on page 2205</a><br><a href="#">show snmp rmon alarms detail on page 2205</a><br><a href="#">show snmp rmon events detail on page 2206</a>                                                                                                                                                                                                                                           |
| <b>Output Fields</b>            | Table 247 describes the output fields for the <b>show snmp rmon</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                            |

Table 247: show snmp rmon Output Fields

| Field Name  | Field Description | Level of Output |
|-------------|-------------------|-----------------|
| Alarm Index | Alarm identifier. | All levels      |

Table 247: show snmp rmon Output Fields (*continued*)

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Level of Output |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>State</b>         | <p>State of the alarm or event entry:</p> <p>Alarms:</p> <ul style="list-style-type: none"> <li>• <b>active</b>—Entry is fully configured and activated.</li> <li>• <b>falling threshold crossed</b>—Value of the variable has crossed the lower threshold limit.</li> <li>• <b>rising threshold crossed</b>—Value of the variable has crossed the upper threshold limit.</li> <li>• <b>under creation</b>—Entry is being configured and is not yet activated.</li> <li>• <b>startup</b>—Alarm is waiting for the first sample of the monitored variable.</li> <li>• <b>object not available</b>—Monitored variable of that type is not available to the SNMP agent.</li> <li>• <b>instance not available</b>—Monitored variable's instance is not available to the SNMP agent.</li> <li>• <b>object type invalid</b>—Monitored variable is not a numeric value.</li> <li>• <b>object processing errored</b>—An error occurred when the monitored variable was processed.</li> <li>• <b>unknown</b>—State is not one of the above.</li> </ul> <p>Events:</p> <ul style="list-style-type: none"> <li>• <b>active</b>—Entry has been fully configured and activated.</li> <li>• <b>under creation</b>—Entry is being configured and is not yet activated.</li> <li>• <b>unknown</b>—State is not one of the above.</li> </ul> | All levels      |
| <b>Variable name</b> | Name of the SNMP object instance being monitored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | All levels      |
| <b>Event Index</b>   | Event identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | All levels      |
| <b>Type</b>          | <p>Type of notification made when an event is triggered. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>log</b>—A system log message is generated and an entry is made to the log table.</li> <li>• <b>snmptrap</b>—An SNMP trap is sent to the configured destination.</li> <li>• <b>log and trap</b>—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination.</li> <li>• <b>none</b>—Neither log nor trap will be sent.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail</b>   |
| <b>Last Event</b>    | Date and time of the last event. It has the format <i>yyyy-mm-dd hh:mm:ss timezone</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>brief</b>    |
| <b>Community</b>     | Identifies the trap group used for sending the SNMP trap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>detail</b>   |
| <b>Variable OID</b>  | Object ID to which the variable name is resolved. The format is x.x.x.x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>detail</b>   |
| <b>Sample type</b>   | Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of <b>absolute value</b> or <b>delta value</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>detail</b>   |

Table 247: show snmp rmon Output Fields (*continued*)

| Field Name                 | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Level of Output |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Startup alarm</b>       | Alarm that might be sent when this entry is first activated, depending on the following criteria: <ul style="list-style-type: none"> <li>Alarm is sent when one of the following situations exists: <ul style="list-style-type: none"> <li>Value of the alarm is above or equal to the rising threshold and the startup type is either <b>rising alarm</b> or <b>rising or falling alarm</b>.</li> <li>Value of the alarm is below or equal to the falling threshold and the startup type is either <b>falling alarm</b> or <b>rising or falling alarm</b>.</li> </ul> </li> <li>Alarm is <i>not</i> sent when one of the following situations exists: <ul style="list-style-type: none"> <li>Value of the alarm is above or equal to the rising threshold and the startup type is <b>falling alarm</b>.</li> <li>Value of the alarm is below or equal to the falling threshold and the startup type is <b>rising alarm</b>.</li> <li>Value of the alarm is between the thresholds.</li> </ul> </li> </ul> | <b>detail</b>   |
| <b>Owner</b>               | Name of the entry configured by the user. If the entry was created through the CLI, the owner has <b>monitor</b> prepended to it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>   |
| <b>Creator</b>             | Mechanism by which the entry was configured ( <b>CLI</b> or <b>SNMP</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>detail</b>   |
| <b>Sample interval</b>     | Time period between samples (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>detail</b>   |
| <b>Rising threshold</b>    | Upper limit threshold value configured by the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Falling threshold</b>   | Lower limit threshold value configured by the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Rising event index</b>  | Event triggered when the rising threshold is crossed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail</b>   |
| <b>Falling event index</b> | Event triggered when the falling threshold is crossed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>detail</b>   |
| <b>Current value</b>       | Current value of the monitored variable in the most recent sample interval.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail</b>   |

## Sample Output

### show snmp rmon

```

user@host> show snmp rmon
Alarm
Index State Variable name
 1 falling threshold crossed ifInOctets.1

Event
Index Type Last Event
 1 log and trap 2002-01-30 01:13:01 PST

```

### show snmp rmon alarms detail

```

user@host> show snmp rmon alarms detail

```

```
Alarm Index 1:
Variable name ifInOctets.1
Variable OID 1.3.6.1.2.1.2.2.1.10.1
Sample type delta value
Startup alarm rising or falling alarm
Owner monitor
Creator CLI
State falling threshold crossed
Sample interval 60 seconds
Rising threshold 100000
Falling threshold 80000
Rising event index 1
Falling event index 1
Current value 0
```

#### show snmp rmon events detail

```
user@host> show snmp rmon events detail
Event Index 1:
Type log and trap
Community boy-elroy
Last event 2002-01-30 01:13:01 PST
Creator CLI
State active
```

## show snmp statistics

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show snmp statistics<br><subagents>                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Option <b>subagents</b> introduced in Junos OS Release 14.2.</p> |
| <b>Description</b>              | Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <b>subagents</b> —(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.                                                                                                                                           |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear snmp statistics on page 2121</a></li> </ul>                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <p><a href="#">show snmp statistics on page 2212</a></p> <p><a href="#">show snmp statistics subagents on page 2212</a></p>                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 248</a> describes the output fields for the <b>show snmp statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                     |

Table 248: show snmp statistics Output Fields

| Field Name   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b> | <p>Information about received packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets(snmplnPkts)</b>—Total number of messages delivered to the SNMP entity from the transport service.</li> <li>• <b>Bad versions—(snmplnBadVersions)</b> Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version.</li> <li>• <b>Bad community names—(snmplnBadCommunityNames)</b> Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity.</li> <li>• <b>Bad community uses—(snmplnBadCommunityUses)</b> Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message.</li> <li>• <b>ASN parse errors—(snmplnASNParseErrs)</b> Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.</li> <li>• <b>Too big—(snmplnTooBigs)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names—(snmplnNoSuchNames)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values—(snmplnBadValues)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>badValue</b>.</li> <li>• <b>Read only—(snmplnReadOnlys)</b> Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of <b>readOnly</b>. Only incorrect implementations of SNMP generate this error.</li> </ul> |



Table 248: show snmp statistics Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Input (continued) | <ul style="list-style-type: none"> <li>• <b>General errors—(snmpInGenErrs)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>genErr</b>.</li> <li>• <b>Total requests varbinds—(snmpInTotalReqVars)</b> Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP <b>GetRequest</b> and <b>GetNext</b> PDUs.</li> <li>• <b>Total set varbinds—(snmpInSetVars)</b> Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP <b>SetRequest</b> PDUs.</li> <li>• <b>Get requests—(snmpInGetRequests)</b> Total number of SNMP <b>GetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get nexts—(snmpInGetNexts)</b> Total number of SNMP <b>GetNext</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Set requests—(snmpInSetRequests)</b> Total number of SNMP <b>SetRequest</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Get responses—(snmpInGetResponses)</b> Total number of SNMP <b>GetResponse</b> PDUs that have been accepted and processed by the SNMP entity.</li> <li>• <b>Traps—(snmpInTraps)</b> Total number of SNMP traps generated by the SNMP entity.</li> <li>• <b>Silent drops—(snmpSilentDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.</li> <li>• <b>Proxy drops—(snmpProxyDrops)</b> Total number of <b>GetRequest</b>, <b>GetNextRequest</b>, <b>GetBulkRequest</b>, <b>SetRequests</b>, and <b>InformRequest</b> PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned.</li> <li>• <b>Commit pending drops</b>—Number of SNMP packets for <b>Set</b> requests dropped because of a previous pending SNMP <b>Set</b> request on the committed configuration.</li> <li>• <b>Throttle drops</b>—Number of SNMP packets for any requests dropped reaching the throttle limit.</li> </ul> |

Table 248: show snmp statistics Output Fields (*continued*)

| Field Name | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V3 Input   | <p>Information about SNMP version 3 packets:</p> <ul style="list-style-type: none"> <li>• <b>Unknown security models—(snmpUnknownSecurityModels)</b> Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine.</li> <li>• <b>Invalid messages—(snmpInvalidMsgs)</b> Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message.</li> <li>• <b>Unknown pdu handlers—(snmpUnknownPDUHandlers)</b> Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type.</li> <li>• <b>Unavailable contexts—(snmpUnavailableContexts)</b> Number of requests received for a context that is known to the SNMP engine, but is currently unavailable.</li> <li>• <b>Unknown contexts—(snmpUnknownContexts)</b> Total number of requests received for a context that is unknown to the SNMP engine.</li> <li>• <b>Unsupported security levels—(usmStatsUnsupportedSecLevels)</b> Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable).</li> <li>• <b>Not in time windows—(usmStatsNotInTimeWindows)</b> Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window.</li> <li>• <b>Unknown user names—(usmStatsUnknownUserNames)</b> Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.</li> <li>• <b>Unknown engine ids—(usmStatsUnknownEngineIDs)</b> Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine.</li> <li>• <b>Wrong digests—(usmStatsWrongDigests)</b> Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.</li> <li>• <b>Decryption errors—(usmStatsDecryptionErrors)</b> Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.</li> </ul> |

Table 248: show snmp statistics Output Fields (*continued*)

| Field Name    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Output</b> | <p>Information about transmitted packets:</p> <ul style="list-style-type: none"> <li>• <b>Packets—(snmpOutPkts)</b> Total number of messages passed from the SNMP entity to the transport service.</li> <li>• <b>Too big—(snmpOutTooBigs)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>tooBig</b>.</li> <li>• <b>No such names—(snmpOutNoSuchNames)</b> Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <b>noSuchName</b>.</li> <li>• <b>Bad values—(snmpOutBadValues)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>badValue</b>.</li> <li>• <b>General errors—(snmpOutGenErrs)</b> Total number of SNMP PDUs generated by the SNMP entity with an error status field of <b>genErr</b>.</li> <li>• <b>Get requests—(snmpOutGetRequests)</b> Total number of SNMP <b>GetRequest</b> PDUs generated by the SNMP entity.</li> <li>• <b>Get nexts—(snmpOutGetNexts)</b> Total number of SNMP <b>GetNext</b> PDUs generated by the SNMP entity.</li> <li>• <b>Set requests—(snmpOutSetRequests)</b> Total number of SNMP <b>SetRequest</b> PDUs generated by the SNMP entity.</li> <li>• <b>Get responses—(snmpOutGetResponses)</b> Total number of SNMP <b>GetResponse</b> PDUs generated by the SNMP entity.</li> <li>• <b>Traps—(snmpOutTraps)</b> Total number of SNMP traps generated by the SNMP entity.</li> </ul> |

Table 249 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 249: show snmp statistics subagents Output Fields

| Field Name                   | Field Description                                                        |
|------------------------------|--------------------------------------------------------------------------|
| <b>Subagent</b>              | Location of the SNMP subagent.                                           |
| <b>Request PDUs</b>          | Number of PDUs requested by the SNMP manager.                            |
| <b>Response PDUs</b>         | Number of response PDUs sent by the SNMP subagent.                       |
| <b>Request Variables</b>     | Number of variable bindings on the PDUs requested by the SNMP manager.   |
| <b>Response Variables</b>    | Number of variable bindings on the PDUs sent by the SNMP subagent.       |
| <b>Average Response Time</b> | Average time taken by the SNMP subagent to send statistics response.     |
| <b>Maximum Response Time</b> | Maximum time taken by the SNMP subagent to send the statistics response. |

## Sample Output

### show snmp statistics

```
user@host> show snmp statistics
SNMP statistics:
 Input:
 Packets: 246213, Bad versions: 12, Bad community names: 12,
 Bad community uses: 0, ASN parse errors: 96,
 Too big: 0, No such names: 0, Bad values: 0,
 Read onlys: 0, General errors: 0,
 Total request varbinds: 227084, Total set varbinds: 67,
 Get requests: 44942, Get nexts: 190371, Set requests: 10712,
 Get responses: 0, Traps: 0,
 Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
 Throttle drops: 0,
 V3 Input:
 Unknown security models: 0, Invalid messages: 0
 Unknown pdu handlers: 0, Unavailable contexts: 0
 Unknown contexts: 0, Unsupported security levels: 1
 Not in time windows: 0, Unknown user names: 0
 Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
 Output:
 Packets: 246093, Too big: 0, No such names: 31561,
 Bad values: 0, General errors: 2,
 Get requests: 0, Get nexts: 0, Set requests: 0,
 Get responses: 246025, Traps: 0
```

### show snmp statistics subagents

```
user@host> show snmp statistics subagents

Subagent: /var/run/cosd-20
 Request PDUs: 0, Response PDUs: 0,
 Request Variables: 0, Response Variables: 0,
 Average Response Time(ms): 0.00,
 Maximum Response Time(ms): 0.00

Subagent: /var/run/pfed-30
 Request PDUs: 0, Response PDUs: 0,
 Request Variables: 0, Response Variables: 0,
 Average Response Time(ms): 0.00,
 Maximum Response Time(ms): 0.00

Subagent: /var/run/rmopd-15
 Request PDUs: 0, Response PDUs: 0,
 Request Variables: 0, Response Variables: 0,
 Average Response Time(ms): 0.00,
 Maximum Response Time(ms): 0.00

Subagent: /var/run/chassisd-30
 Request PDUs: 33116, Response PDUs: 33116,
 Request Variables: 33116, Response Variables: 33116,
 Average Response Time(ms): 1.83,
 Maximum Response Time(ms): 203.48

Subagent: /var/run/pkid-13
 Request PDUs: 0, Response PDUs: 0,
 Request Variables: 0, Response Variables: 0,
 Average Response Time(ms): 0.00,
 Maximum Response Time(ms): 0.00
```

Subagent: /var/run/apsd-13  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33  
Request PDUs: 74211, Response PDUs: 74211,  
Request Variables: 74211, Response Variables: 74211,  
Average Response Time(ms): 2.30,  
Maximum Response Time(ms): 51.04

Subagent: /var/run/license-check-16  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd\_snmp  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18  
Request PDUs: 0, Response PDUs: 0,  
Request Variables: 0, Response Variables: 0,  
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00



## show snmp stats-response-statistics

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show snmp stats-response-statistics                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.2.                                                                                                                              |
| <b>Description</b>              | Display statistics of SNMP statistics responses sent from the Packet Forwarding Engine during the MIB II process (mib2d).                                                 |
| <b>Options</b>                  | This command has no options.                                                                                                                                              |
| <b>Required Privilege Level</b> | view                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show snmp stats-response-statistics on page 2215</a>                                                                                                          |
| <b>Output Fields</b>            | Table 250 describes the output fields for the <b>show snmp stats-response-statistics</b> command. Output fields are listed in the approximate order in which they appear. |

Table 250: show snmp stats-response-statistics Output Fields

| Field Name                              | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Average response time statistics</b> | <p>Display the average response time in milliseconds per protocol data unit (PDU) by snmpd. It includes the following information:</p> <ul style="list-style-type: none"> <li>• <b>Stats Type</b>—Type of SNMP statistics.</li> <li>• <b>Stats Responses</b>—Number of SNMP statistics responses received from the Packet Forwarding Engine.</li> <li>• <b>Average Response Time</b>—Average time taken to receive the statistics response from the Packet Forwarding Engine in milliseconds.</li> </ul>                                |
| <b>Bucket statistics</b>                | <p>Information about SNMP statistics responses:</p> <ul style="list-style-type: none"> <li>• <b>Bucket Type</b>—Category of time intervals in which SNMP statistics responses are received from the Packet Forwarding Engine.</li> <li>• <b>Stats Responses</b>—Number of SNMP statistics responses received from the Packet Forwarding Engine.</li> </ul>                                                                                                                                                                              |
| <b>Bad responses</b>                    | <p>Information about top 20 bad responses from a subagent:</p> <ul style="list-style-type: none"> <li>• <b>Response</b>—Time taken to receive the SNMP statistics response from the Packet Forwarding Engine in milliseconds.</li> <li>• <b>Request Time</b>—Date and time of SNMP request.</li> <li>• <b>Key</b>—Display the attribute of SNMP <b>Stats Type</b>. For example, in the case of SNMP statistics responses for interfaces, the Key value is SNMP ifIndex, and for firewalls, the Key value is the filter name.</li> </ul> |

## Sample Output

### show snmp stats-response-statistics

```

user@host> show snmp stats-response-statistics
Average response time statistics:
Stats Stats Average

```

| Type        | Responses | Response<br>Time (ms) |
|-------------|-----------|-----------------------|
| ifd(non ae) | 34182     | 175.48                |
| ifd(ae)     | 0         | 0.00                  |
| ifl(non ae) | 5472      | 5.40                  |
| ifl(ae)     | 0         | 0.00                  |
| firewall    | 15        | 1141.73               |

## Bucket statistics:

| Bucket<br>Type(ms) | Stats<br>Responses |
|--------------------|--------------------|
| 0 - 10             | 39078              |
| 11 - 50            | 588                |
| 51 - 100           | 0                  |
| 101 - 200          | 0                  |
| 201 - 500          | 1                  |
| 501 - 1000         | 2                  |
| 1001 - 2000        | 0                  |
| 2001 - 5000        | 0                  |
| More than 5001     | 0                  |

## Bad responses:

| Response<br>Time<br>(ms) | Request<br>Time<br>(UTC) | Stats<br>Type | Key                     |
|--------------------------|--------------------------|---------------|-------------------------|
| 927.80                   | 2014-03-26 05:44:16      | firewall      | __default_arp_policer__ |
| 908.68                   | 2014-03-26 05:44:16      | firewall      | __default_bpdu_filter__ |
| 421.00                   | 2014-03-26 05:46:25      | ifd(non ae)   | 504                     |
| 49.76                    | 2014-04-13 04:15:18      | ifd(non ae)   | 503                     |
| 49.62                    | 2014-04-13 04:30:18      | ifd(non ae)   | 504                     |
| 48.52                    | 2014-04-05 10:06:55      | ifd(non ae)   | 504                     |
| 47.61                    | 2014-04-11 04:06:27      | ifd(non ae)   | 505                     |
| 47.38                    | 2014-04-13 03:30:18      | ifd(non ae)   | 501                     |
| 47.22                    | 2014-03-27 20:08:07      | ifd(non ae)   | 502                     |
| 46.26                    | 2014-03-31 13:08:58      | ifd(non ae)   | 506                     |
| 46.00                    | 2014-04-13 04:00:18      | ifd(non ae)   | 503                     |
| 45.95                    | 2014-04-05 17:15:17      | ifd(non ae)   | 503                     |
| 45.75                    | 2014-04-15 13:06:10      | ifd(non ae)   | 507                     |
| 45.60                    | 2014-04-01 03:07:28      | ifd(non ae)   | 517                     |
| 45.56                    | 2014-04-08 13:09:15      | ifd(non ae)   | 502                     |
| 45.23                    | 2014-04-13 03:15:18      | ifd(non ae)   | 501                     |
| 45.15                    | 2014-04-05 16:45:17      | ifd(non ae)   | 501                     |
| 44.74                    | 2014-04-08 22:08:47      | ifd(non ae)   | 505                     |
| 44.10                    | 2014-04-05 16:30:17      | ifd(non ae)   | 501                     |
| 44.00                    | 2014-04-08 09:09:23      | ifd(non ae)   | 524                     |



## show snmp v3

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show snmp v3</code><br><code>&lt;access &lt;brief   detail&gt;   community   general   groups   notify &lt;filter&gt;   target &lt;address   parameters&gt;   users&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display the Simple Network Management Protocol version 3 (SNMPv3) operating configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>none</b>—Display all of the SNMPv3 operating configuration.</p> <p><b>access</b>—(Optional) Display SNMPv3 access information.</p> <p><b>brief   detail</b>—(Optional) Display brief or detailed information about SNMPv3 access information.</p> <p><b>community</b>—(Optional) Display SNMPv3 community information.</p> <p><b>general</b>—(Optional) Display SNMPv3 general information.</p> <p><b>groups</b>—(Optional) Display SNMPv3 security-to-group information.</p> <p><b>notify &lt;filter&gt;</b>—(Optional) Display SNMPv3 notify and, optionally, notify filter information.</p> <p><b>target &lt;address   parameters&gt;</b>—(Optional) Display SNMPv3 target and, optionally, either target address or target parameter information.</p> <p><b>users</b>—(Optional) Display SNMPv3 user information.</p> |
| <b>Additional Information</b>   | To edit the default display of the <b>show snmp v3</b> command, specify options in the <b>show</b> statement at the <b>[edit snmp v3]</b> hierarchy level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show snmp v3 on page 2219</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | <a href="#">Table 251</a> describes the output fields for the <b>show snmp v3</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 251: show snmp v3 Output Fields

| Field Name            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access control</b> | <p>Information about access control:</p> <ul style="list-style-type: none"> <li>• <b>Group</b>—Group name for which the configured access privileges apply. The group, together with the context prefix and the security model and security level, forms the index for this table.</li> <li>• <b>Context prefix</b>—SNMPv3 context for which the configured access privileges apply.</li> <li>• <b>Security model/level</b>—Security model and security level for which the configuration access privileges apply.</li> <li>• <b>Read view</b>—Identifies the MIB view applied to SNMPv3 read operations.</li> <li>• <b>Write view</b>—Identifies the MIB view applied to SNMPv3 write operations.</li> <li>• <b>Notify view</b>—Identifies the MIB view applied to outbound SNMP notifications.</li> </ul>                                                                                                                                                                                                                                       |
| <b>Engine</b>         | <p>Information about local engine configuration:</p> <ul style="list-style-type: none"> <li>• <b>Local engine ID</b>—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.</li> <li>• <b>Engine boots</b>—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.</li> <li>• <b>Engine time</b>—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.</li> <li>• <b>Max msg size</b>—Maximum message size the sender can accommodate.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Engine ID</b>      | <p>Information about engine ID:</p> <ul style="list-style-type: none"> <li>• <b>Local engine ID</b>—Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.</li> <li>• <b>Engine boots</b>—Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.</li> <li>• <b>Engine time</b>—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.</li> <li>• <b>Max msg size</b>—Maximum message size the sender can accommodate.</li> <li>• <b>Engine ID</b>—SNMPv3 engine ID associated with each user.</li> <li>• <b>User</b>—SNMPv3 user.</li> <li>• <b>Auth/Priv</b>—Authentication and encryption algorithm available for use by each user.</li> <li>• <b>Storage</b>—Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.</li> <li>• <b>Status</b>—Status of the conceptual row. Only rows with an active status are used by the SNMPv3 engine.</li> </ul> |
| <b>Group name</b>     | Name of the group to which this entry belongs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Security model</b> | Identifies the security model context for the security name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Security name</b>  | Used with the security model; identifies a specific security name instance. Each security model/security name combination can be assigned to a specific group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Storage type</b>   | Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Status</b>         | Status of the conceptual row. Only rows with active status are used by the SNMPv3 engine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Sample Output

### show snmp v3

```

user@host> show snmp v3
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots: 38
Engine time: 64583 seconds
Max msg size: 2048 bytes

Engine ID: local
 User Auth/Priv Storage Status
 user1 md5/des nonvolatile active
 user2 sha/none nonvolatile active
 user3 none/none nonvolatile active

Engine ID: 81 00 0a 4c 04 64 64 64 64
 User Auth/Priv Storage Status
 UNEW md5/none nonvolatile active
Group name Security model Security name Storage type Status
g1 usm user1 nonvolatile active
g2 usm user2 nonvolatile active
g3 usm user3 nonvolatile active

Access control:
Group Context prefix Security model/level Read view Write view Notify view
g1 usm/privacy v1 v1
g2 usm/authent v1 v1
g3 usm/none v1 v1

```

## show system alarms

---

|                                 |                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system alarms                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for SRX Series devices.                                                                                                                                                                                          |
| <b>Description</b>              | Display active system alarms.                                                                                                                                                                                                                                |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                                 |
| <b>Additional Information</b>   | System alarms are preset. They include a <b>configuration</b> alarm that appears when no rescue configuration alarm is set and a <b>license</b> alarm that appears when a software feature is configured but no valid license is configured for the feature. |
| <b>Required Privilege Level</b> | admin                                                                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show system alarms on page 2220</a>                                                                                                                                                                                                              |

## Sample Output

### show system alarms

```
user@host> show system alarms
5 alarms currently active
Alarm time Class Description
2012-05-29 16:47:18 UTC Major /var partition usage crossed critical threshold
2012-05-29 16:47:18 UTC Minor /var partition usage crossed high threshold
2012-05-29 16:47:18 UTC Major /root partition usage crossed critical threshold
2012-05-29 16:47:18 UTC Minor /root partition usage crossed high threshold
2012-05-29 16:47:18 UTC Minor Rescue configuration is not set
```

## show system resource-monitor fpc

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show system resource-monitor fpc slot-number</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX80, MX104, MX240, MX480, MX960, MX2010, and MX2020 routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Display the utilization of memory resources on the Packet Forwarding Engines of an FPC. The filter memory denotes the filter counter memory used for firewall filter counters. The asterisk (*) displayed next to each of the memory regions denotes the ones for which the configured threshold is being currently exceeded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>fpc slot-number</b>—Display the Junos OS utilization information of memory resources for the specified slot number in which the FPC is installed.</p> <ul style="list-style-type: none"> <li>MX80 router—Replace <b>fpc-slot</b> with a value from 1. This command is not supported on FPC slot 0.</li> <li>MX104 router—Replace <b>fpc-slot</b> with a value from 0 through 2.</li> <li>MX240 router—Replace <b>fpc-slot</b> with a value from 0 through 2.</li> <li>MX480 router—Replace <b>fpc-slot</b> with a value from 0 through 5.</li> <li>MX-960 router—Replace <b>fpc-slot</b> with a value from 0 through 11.</li> <li>MX2010 router—Replace <b>fpc-slot-number</b> with a value from 0 through 9.</li> <li>MX2020 router—Replace <b>fpc-slot-number</b> with a value from 0 through 19.</li> </ul> |
| <b>Additional Information</b>   | The filter memory denotes the filter counter memory used for firewall filter counters. From the Ukern perspective, MPC5E contains only one Packet Forwarding Engine instance. The <b>show chassis fabric plane</b> command output displays the state of fabric plane connections to the Packet Forwarding Engine. Because two Packet Forwarding Engines exist, you notice PFE-0 and PFE-1 in the output.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>List of Sample Output</b>    | <a href="#">show system resource-monitor fpc on page 2222</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | Table 252 lists the output fields for the <b>show system resource-monitor fpc</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 252: show system resource-monitor fpc Output Fields

| Field Name                 | Field Description                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Free Heap Memory Watermark | Configured watermark value for the percentage of free memory space used for ukernel or heap memory to be monitored    |
| Free FW Memory Watermark   | Configured watermark value for the percentage of free memory space used for firewall or filter memory to be monitored |

Table 252: show system resource-monitor fpc Output Fields (*continued*)

| Field Name               | Field Description                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Free NH Memory Watermark | Configured watermark value for the percentage of free memory space used for next-hop memory to be monitored                                        |
| * - watermark reached    | An asterix (*) displayed beside any of the memory regions denotes the memory types for which the configured threshold is being currently exceeded. |
| Slot #                   | Slot number in which the line card is installed                                                                                                    |
| PFE #                    | Number or identifier of the Packet Forwarding Engine in the specified line card slot                                                               |
| Heap % free              | Percentage of free space associated with heap or ukernel memory                                                                                    |
| Encap mem % free         | Percentage of free space associated with encapsulation memory                                                                                      |
| NH mem % free            | Percentage of free space associated with next-hop memory                                                                                           |
| Filter / FW mem % free   | Percentage of free space associated with firewall or filter memory                                                                                 |

## Sample Output

### show system resource-monitor fpc

```

user@host> show system resource-monitor fpc
FPC Resource Usage Summary

Free Heap Mem Watermark : 20 %
Free NH Mem Watermark : 20 %
Free Filter Mem Watermark : 20 %

* - Watermark reached

mem
Slot # Heap ENCAP mem NH mem FW
 % Free PFE # % Free % Free % Free
 0 0 NA 83
 99

```

# Standards Reference





## PART 26

# Overview

- [Accessing Standards Documents on page 2227](#)



# Accessing Standards Documents

- Accessing Standards Documents on the Internet on page 2227

## Accessing Standards Documents on the Internet

---

The following information about the location of standards on the Internet is accurate as of February 2011. It is subject to change and is provided only as a courtesy to the reader.

Information about accessing MIBs is provided in the entry for each MIB.

- ANSI standards are published by the American National Standards Institute. You can search for specific standards at <http://webstore.ansi.org>.
- FRF (Frame Relay Forum) standards are published by the Broadband Forum. They can be accessed at <http://www.broadband-forum.org/technical/ipmplstechspec.php>.
- GR (Generic Requirements) standards are published by Telcordia. Information about them can be accessed by clicking the “Document Center” link at <http://telecom-info.telcordia.com/site-cgi/ido/>.
- IEEE standards are published by the Institute of Electrical and Electronics Engineers. They can be accessed at <http://standards.ieee.org/getieee802/index.html>.
- ISO/IEC standards are published by the International Organization for Standardization/International Electrotechnical Commission. They can be accessed at [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/](http://www.iso.org/iso/iso_catalogue/catalogue_tc/).
- INCITS standards are published by the InterNational Committee for Information Technology Standards. They can be accessed at <https://standards.incits.org/>.
- Internet drafts are published by the Internet Engineering Task Force (IETF). They can be accessed at <http://tools.ietf.org/id/>.
- ITU–T Recommendations are published by the International Telecommunication Union. They can be accessed at <http://www.itu.int/rec/T-REC>.



**NOTE:** Junos OS supports ITU-T Y.1731 (year 2006 version) that defines Ethernet service OAM features for fault monitoring, diagnostics, and performance monitoring.

- RFCs are published by the IETF. They can be accessed at <http://www.ietf.org/rfc.html>.



## PART 27

# Supported Standards

- [Chassis and System Standards on page 2231](#)
- [Interface Standards on page 2247](#)
- [Layer 2 Standards on page 2253](#)
- [MPLS Applications Standards on page 2257](#)
- [Open Standards on page 2265](#)
- [Packet Processing Standards on page 2269](#)
- [Routing Protocol Standards on page 2273](#)
- [Services PIC and DPC Standards on page 2287](#)
- [VPLS and VPN Standards on page 2293](#)



# Chassis and System Standards

- [Supported BFD Standards on page 2231](#)
- [Supported BOOTP and DHCP Standards on page 2232](#)
- [Supported Mobile IP Standards on page 2233](#)
- [Supported Network Management Standards on page 2233](#)
- [Supported RADIUS and TACACS+ Standards for User Authentication on page 2244](#)
- [Supported System Access Standards on page 2244](#)
- [Supported Time Synchronization Standard on page 2245](#)

## Supported BFD Standards

---

Junos OS substantially supports the following standards for Bidirectional Forwarding Detection (BFD).

- RFC 5880, *Bidirectional Forwarding Detection*. (Partial support—Echo and Demand mode is not supported).
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6* (Fully compliant).
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*.
- RFC 5883, *Bidirectional Forwarding Detection (BFD)* (Fully compliant).
- RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*. (Partial support—Packets from egress to ingress come with singlehop port and while sending packets, the router alert option is used setting TTL to 1).
- RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. (Fully compliant)

## Supported BOOTP and DHCP Standards

---

The Junos operating system (Junos OS) substantially supports the following RFCs, which define standards for the bootstrap protocol (BOOTP) and the Dynamic Host Control Protocol (DHCP).

- RFC 951, *BOOTSTRAP PROTOCOL (BOOTP)*
- RFC 1001, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS*
- RFC 1002, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS*
- RFC 1035, *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*
- RFC 1534, *Interoperation Between DHCP and BOOTP*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 1700, *ASSIGNED NUMBERS*
- RFC 2131, *Dynamic Host Configuration Protocol*

DHCP over virtual LAN (VLAN)-tagged interfaces is not supported.

- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3118, *Authentication for DHCP Messages*

Only Section 4, "Configuration token," is supported.

- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*
- RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*
- RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)*
- RFC 4649, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)



## Supported Mobile IP Standards

---

Junos OS supports only static configuration of home agent addresses and IP tunnels; dynamic configuration is not supported. Junos OS does not support the Mobile IP foreign agent, accounting, QoS, policy, data path, or logical interfaces per mobile node (for a mobile subscriber).

Junos OS substantially supports the following RFCs, which define standards for Mobile IP.

- RFC 2794, *Mobile IP Network Access Identifier Extension for IPv4*
- RFC 3024, *Reverse Tunneling for Mobile IP, revised*
- RFC 3344, *IP Mobility Support for IPv4*

Only the Mobile IP home agent is supported.

- RFC 3543, *Registration Revocation in Mobile IPv4*
- RFC 4433, *Mobile IPv4 Dynamic Home Agent (HA) Assignment*

The following RFC does not define a standard, but provides information about Mobile IP. The IETF classifies it as “Informational.”

- RFC 2977, *Mobile IP Authentication, Authorization, and Accounting Requirements*  
Accounting is not supported.

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Network Management Standards

---

Junos OS supports the majority of network management features defined in the following standards documents.

- Extended Security Options (ESO) Consortium, *ESO Consortium MIB*.

As of February 2011, the text of this MIB is accessible at  
<http://www.snmp.com/eso/esoConsortiumMIB.txt>.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)

Only the following MIB objects are supported:

- **dot3adAggPortDebugActorChangeCount**
- **dot3adAggPortDebugActorSyncTransitionCount**
- **dot3adAggPortDebugMuxState**
- **dot3adAggPortDebugPartnerChangeCount**

- dot3adAggPortDebugPartnerSyncTransitionCount
  - dot3adAggPortDebugRxState
  - dot3adAggPortListTable
  - dot3adAggPortStatsTable
  - dot3adAggPortTable
  - dot3adAggTable
  - dot3adTablesLastChanged
- Integrated Local Management Interface (ILMI) MIB in the *Integrated Local Management Interface (ILMI) Specification, Version 4.0*.

As of February 2011, this document is accessible at

<http://www.broadband-forum.org/ftp/pub/approved-specs/af-ilmi-0065.000.pdf>.

Only the atmfMYIPNmAddress and atmfPortMyIfname objects are supported.

- Internet Assigned Numbers Authority (IANA), *IANAiftype Textual Convention MIB* (referenced by RFC 2863, *The Interfaces Group MIB*)

As of February 2011, the text of this MIB is accessible at

<http://www.iana.org/assignments/ianaiftype-mib>.

- RFC 1122, *Requirements for Internet Hosts -- Communication Layers*
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1156, *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

Only the following MIB objects are supported:

- isisAdjIPAddr
- isisAreaAddr
- isisCirc
- isisCircLevel
- isisIPRA
- isisISAdj
- isisISAdjAreaAddr
- isisISAdjProtSupp
- isisMANAreaAddr
- isisPacketCount
- isisRa

- **isisSysProtSupp**
- **isisSummAddr**
- **isisSystem**
- RFC 1212, *Concise MIB Definitions*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*

Only the following features are supported:

- Junos OS-specific secured access list
- Master configuration keywords
- MIB II and its SNMP version 2 derivatives, including the following:
  - Interface management
  - IP (except for the **ipRouteTable** object, which has been replaced by the **inetCidrRouteTable** object, [RFC 4292, *IP Forwarding MIB*])
  - SNMP management
  - Statistics counters
- Reconfigurations upon receipt of the SIGHUP signal
- SNMP version 1 **Get** and **GetNext** requests and version 2 **GetBulk** requests
- RFC 1215, *A Convention for Defining Traps for use with the SNMP*

Only MIB II SNMP version 1 traps and version 2 notifications are supported.

- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* (obsoleted by RFC 2495)

The T1 MIB is supported.

- RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type* (obsoleted by RFC 2496)

The T3 MIB is supported.

- RFC 1472, *The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol*
- RFC 1473, *The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol*
- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*

The **bgpBackwardTransition** and **bgpEstablished** notifications are not supported.

- RFC 1695, *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2* (obsoleted by RFC 2515)
- RFC 1724, *RIP Version 2 MIB Extension*

- RFC 1850, *OSPF Version 2 Management Information Base*

The following features are not supported:

- Host Table
- **ospfLsdbApproachingOverflow** trap
- **ospfLsdbOverflow** trap
- **ospfOriginateLSA** trap
- **ospfOriginateNewLsas** MIB object
- **ospfRxNewLsas** MIB object
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3416)
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3418)
- RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*
- RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2*
- RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*
- RFC 2068, *Hypertext Transfer Protocol -- HTTP/1.1*
- RFC 2096, *IP Forwarding Table MIB*

The **ipCidrRouteTable** object is extended to include the tunnel name when the next hop is through an RSVP-signaled label-switched path (LSP).



**NOTE:** RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.

---

- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*
- RFC 2233, *The Interfaces Group MIB using SMIv2* (obsoleted by RFC 2863)
- RFC 2287, *Definitions of System-Level Managed Objects for Applications*

Only the following MIB objects are supported:

- **sysAppElmtRunTable**
- **sysApplInstallElmtTable**
- **sysApplInstallPkgTable**
- **sysApplMapTable**

- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2466, *Management Information Base for IP Version 6: ICMPv6 Group*
- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types*

The following MIB objects are not supported:

- **dsx1FarEndConfigTable**
  - **dsx1FarEndCurrentTable**
  - **dsx1FarEndIntervalTable**
  - **dsx1FarEndTotalTable**
  - **dsx1FracTable**
- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type*

The following MIB objects are not supported:

- **dsx3FarEndConfigTable**
  - **dsx3FarEndCurrentTable**
  - **dsx3FarEndIntervalTable**
  - **dsx3FarEndTotalTable**
  - **dsx3FracTable**
- RFC 2515, *Definitions of Managed Objects for ATM Management*

The following MIB objects are not supported:

- **aal5VccTable**
  - **atmVcCrossConnectTable**
  - **atmVpCrossConnectTable**
- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type* (obsoleted by RFC 3592)
  - RFC 2571, *An Architecture for Describing SNMP Management Frameworks*  
Only read-only access is supported.
  - RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (obsoleted by RFC 3412)  
Only read-only access is supported.
  - RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
  - RFC 2579, *Textual Conventions for SMIv2*

- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2662, *Definitions of Managed Objects for the ADSL Lines*
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

The following features are not supported:

- Row creation
- **Set** operation
- **vrpStatsPacketLengthErrors** MIB object
- RFC 2790, *Host Resources MIB*

Only the following MIB objects are supported:

- **hrStorageTable** object. The file systems **/**, **/config**, **/var**, and **/tmp** always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.
- Objects in the **hrSystem** group.
- Objects in the **hrSWInstalled** group.
- RFC 2819, *Remote Network Monitoring Management Information Base*

Only the following MIB objects are supported:

- **alarmTable**
- **etherStatsTable** object for Ethernet interfaces
- **eventTable**
- **logTable**
- RFC 2863, *The Interfaces Group MIB*
- RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*
- RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*

Only the following MIB objects are supported:

- **pingCtlTable**
- **pingMaxConcurrentRequests**
- **pingProbeHistoryTable**
- **pingResultsTable**
- **traceRouteCtlTable**
- **traceRouteHopsTable**

- **traceRouteProbeHistoryTable**
- **traceRouteResultsTable**
- RFC 2932, *IPv4 Multicast Routing MIB*
- RFC 2981, *Event MIB*
- RFC 3014, *Notification Log MIB*
- RFC 3019, *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*
- RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
- RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
- RFC 3413, *Simple Network Management Protocol (SNMP) Applications*

The proxy MIB is not supported.

- RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
- RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
- RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

Support is implemented under the Juniper Networks Enterprise branch.

- RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*
- RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

Supports all objects, except **dot3StatsRateControlAbility** and **dot3StatsRateControlStatus** in **dot3StatsEntry** table.



**NOTE:** The values of the following objects in **dot3HCStatsEntry** table will be always zero for both 32-bit counters and 64-bit counters:

- **dot3HCStatsSymbolErrors**
- **dotHCStatsInternalMacTransmitErrors**

- RFC 3811, *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*
- RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)*

Only read-only access is supported, and the following features and MIB objects are not supported:

- MPLS tunnels as interfaces
- **mplsTunnelCRLDResTable** object
- **mplsTunnelPerfTable** object
- The following objects in the **TunnelResource** table:
  - **mplsTunnelResourceExBurstSize**
  - **mplsTunnelResourceMaxBurstSize**
  - **mplsTunnelResourceMeanBurstSize**
  - **mplsTunnelResourceMeanRate**
  - **mplsTunnelResourceWeight**

The **mplsTunnelCHopTable** object is supported on ingress routers only.



**NOTE:** The branch used by the proprietary LDP MIB (**ldpmib.mib**) conflicts with RFC 3812. **ldpmib.mib** has been deprecated and replaced by **jnx-mpls-ldp.mib**.

- RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*

Only read-only access is supported, and the following MIB objects are not supported:

- **mplsInSegmentMapTable**
- **mplsInSegmentPerfTable**
- **mplsInterfacePerfTable**
- **mplsOutSegmentPerfTable**
- **mplsXCDown**
- **mplsXCUp**
- RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*

Only the following MIB objects are supported:

- **mplsLdpLsrID**
- **mplsLdpSesPeerAddrTable**



- RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

- RFC 4087, *IP Tunnel MIB*

Supports MIB objects with **MAX-ACCESS** of read-only in the following tables:

- **tunnelIfTable**
- **tunnelInetConfigTable**

- RFC 4133, *Entity MIB*

Supports tables and objects except:

- **entityLogicalGroup** table
- **entPhysicalMfgDate** and **entPhysicalUris** objects in **entityPhysical2Group** table
- **entLPMappingTable** and **entPhysicalContainsTable** in **entityMappingGroup** table
- **entityNotificationsGroup** table



**NOTE:** Supported only on MX240, MX480, and MX960 routers.

- RFC 4188, *Definitions of Managed Objects for Bridges*
- RFC 4268, *Entity State MIB*



**NOTE:** Supported only on MX240, MX480, and MX960 routers.

- RFC 4292, *IP Forwarding MIB*

Supports the following table and associated MIB objects:

- **inetCidrRouteTable**
- **inetCidrRouteNumber**
- **inetCidrRouteDiscards**

- RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB*

Supports the following scalar objects and tables:

- **mplsL3VpnConfiguredVrfs**
- **mplsL3VpnActiveVrfs**
- **mplsL3VpnConnectedInterfaces**
- **mplsL3VpnNotificationEnable**
- **mplsL3VpnVrfConfMaxPossRts**
- **mplsL3VpnVrfConfRteMxThrshTime**
- **mplsL3VpnIlliLbIRcvThrsh**

- **mplsL3VpnVrfTable**
- **mplsL3VpnVrfPerfTable**
- **mplsL3VpnVrfRteTable**
- **mplsVpnVrfRTTable**
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

The following features are not supported:

- Row creation
- **Set** operation
- **vrrpv3StatisticsPacketLengthErrors** MIB object
- **vrrpv3StatisticsRowDiscontinuityTime** MIB object
- Internet draft draft-ietf-bfd-mib-02.txt, *Bidirectional Forwarding Detection Management Information Base*

Only read-only access is supported, and the **bfdSessDown** and **bfdSessUp** traps are supported. Objects in the **bfdSessMapTable** and **bfdSessPerfTable** tables are not supported. The MIB that supports this draft is **mib-jnx-bfd-exp.txt** under the Juniper Networks Enterprise **jnxExperiment** branch.

- RFC 4273, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version*

Only the following MIB objects are supported:

- **jnxBgpM2PrefixInPrefixes**
- **jnxBgpM2PrefixInPrefixesAccepted**
- **jnxBgpM2PrefixInPrefixesRejected**
- RFC 4444, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

Only the following tables are supported:

- **isisISAdjAreaAddrTable**
- **isisISAdjIPAddrTable**
- **isisISAdjProtSuppTable**
- **isisISAdjTable**
- RFC 5601, *Pseudowire (PW) Management Information Base (MIB)*
- RFC 5603, *Ethernet Pseudowire (PW) Management Information Base (MIB)*
- Internet draft draft-ietf-msdp-mib-08.txt, *Multicast Source Discovery protocol MIB*

The following MIB objects are not supported:

- **msdpBackwardTransition**
- **msdpEstablished**
- **msdpRequestsTable**
- Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, *Management Information Base for OSPFv3*

Only read-only access is supported, and only for the **ospfv3NbrTable** table. The MIB that supports this draft is **mib-jnx-ospfv3mib.txt** under the Juniper Networks Enterprise **jnxExperiment** branch; MIB object names are prefixed with **jnx** (for example, **jnxOspfv3NbrAddressType**).

- Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode*

The following RFCs do not define standards, but provide information about network management. The IETF classifies them variously as "Best Current Practice," "Experimental" or "Informational."

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 2330, *Framework for IP Performance Metrics*
- RFC 2934, *Protocol Independent Multicast MIB for IPv4*
- RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*
- RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 5601, *PW-FRAME-MIB*

Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.

- RFC 5603, *PWE3 MIB*

Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.

- Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*

Implemented under the Juniper Networks enterprise branch [**jnxExperiment**]. OID for **jnxMvpnExperiment** is **.1.3.6.1.4.1.2636.5.12**. This includes **jnxMvpnNotifications** traps.

#### Related Documentation

- *Network Management Administration Guide for Routing Devices*
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported RADIUS and TACACS+ Standards for User Authentication

---

For validation of the identity of users who attempt to access a router, Junos OS supports RADIUS authentication, TACACS+ authentication, and authentication by means of Junos OS user accounts configured on the router. Junos OS supports the configuration of Juniper Networks-specific RADIUS and TACACS+ attributes, and the creation of template accounts.

All users who can log in to the router must already be assigned to a Junos OS login class. A *login class* defines its members' access privileges during a login session, the commands they can and cannot issue, the configuration statements they can and cannot view or change, and the idle time before a member's login session is terminated.

Junos OS substantially supports the following RFCs, which define standards for RADIUS and TACACS+.

- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 3162, *RADIUS and IPv6*
- RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

The following Internet drafts do not define standards, but provide information about RADIUS. The IETF classifies them as "Informational."

- RFC 2866, *RADIUS Accounting*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

### Related Documentation

- [Supported System Access Standards on page 2244](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported System Access Standards

---

Junos OS substantially supports the following protocols and applications for remote access to routers: telnet, FTP, rlogin, and finger. In addition, the Canada and U.S. version of Junos OS substantially supports SSH as an access protocol.

Junos OS substantially supports RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*.

The Canada and U.S. version of Junos OS substantially supports the following RFCs, which define standards for technologies used with Secure Sockets Layer (SSL).

- RFC 1319, *The MD2 Message-Digest Algorithm*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 2246, *The TLS Protocol Version 1.0*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

The following RFCs provide information about TFTP, which Junos OS supports as a remote access protocol. The IETF does not include the RFCs in its Standards track, instead assigning them status “Unknown (Legacy Stream.)”

- RFC 783, *THE TFTP PROTOCOL (REVISION 2)*
- RFC 906, *Bootstrap Loading using TFTP*

**Related  
Documentation**

- [Supported RADIUS and TACACS+ Standards for User Authentication on page 2244](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported Time Synchronization Standard

Junos OS substantially supports RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*, does not define a standard, but provides information about time synchronization technology. The IETF classifies it as “Informational.”

In CLI operational mode, you can set the current date and time on the router manually or from an NTP server.

On MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP, Junos OS substantially supports RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

**Related  
Documentation**

- [Accessing Standards Documents on the Internet on page 2227](#)



# Interface Standards

- [Supported ATM Interface Standards on page 2247](#)
- [Supported Ethernet Interface Standards on page 2248](#)
- [Supported Frame Relay Interface Standards on page 2249](#)
- [Supported GRE and IP-IP Interface Standards on page 2249](#)
- [Supported PPP Interface Standards on page 2250](#)
- [Supported SDH and SONET Interface Standards on page 2251](#)
- [Supported Serial Interface Standards on page 2252](#)
- [Supported T3 Interface Standard on page 2252](#)

## Supported ATM Interface Standards

---

Junos OS substantially supports the following standards for Asynchronous Transfer Mode (ATM) interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation I.432.3, *B-ISDN user-network interface - Physical layer specification: 1544 kbit/s and 2048 kbit/s operation*
- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*  
Only routed protocol data units (PDUs) are supported.
- RFC 2225, *Classical IP and ARP over ATM*  
Only responses are supported.
- RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*  
Only routed PDUs and Ethernet bridged PDUs are supported.
- RFC 4717, *Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Ethernet Interface Standards

---

Junos OS substantially supports the following standards for Ethernet interfaces.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ag, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management*
- IEEE Standard 802.1ah, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 7: Provider Backbone Bridges*
- IEEE Standard 802.1Q, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks*
- IEEE Standard 802.1Qaz, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Enhanced Transmission Selection*
- IEEE Standard 802.1Qbb, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Priority-based Flow Control*
- IEEE Standard 802.1s, *IEEE Standard for Multiple Instances of Spanning Tree Protocol (MSTP)---Virtual Bridged Local Area Networks*
- IEEE Standard 802.3, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- IEEE Standard 802.3ab, *1000BASE-T* (published as Clause 40 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ae, *10-Gigabit Ethernet* (published as Clauses 44-53 in Section 4 of the 802.3 specification)
- IEEE Standard 802.3ah, *Operations, Administration, and Maintenance (OAM)* (published as Clause 57 in Section 5 of the 802.3 specification)
- IEEE Standard 802.3z, *1000BASE-X* (published as Clauses 34-39, 41-42 in Section 3 of the 802.3 specification)
- InterNational Committee for Information Technology Standards (INCITS) T11, *Fibre Channel Interfaces*
- International Telecommunication Union—Telecommunication Standardization (ITU-T) Recommendation Y.1731, *OAM functions and mechanisms for Ethernet based networks*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)



## Supported Frame Relay Interface Standards

Junos OS substantially supports the following standards for Frame Relay interfaces.

- American National Standards Institute (ANSI), *Annex D, Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames* to T1.617-1991, *Integrated Services Digital Network (ISDN)—Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)*
- Broadband Forum standard FRF.12, *Frame Relay Fragmentation Implementation Agreement*
- FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*
- FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*
- International Telecommunication Union—Telecommunication Standardization (ITU-T), *Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management (using Unnumbered Information frames)* to Recommendation Q.933, *ISDN Digital Subscriber Signalling System No. 1 (DSS1) - Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*
- RFC 1973, *PPP in Frame Relay*
- RFC 2390, *Inverse Address Resolution Protocol*
- RFC 2427, *Multiprotocol Interconnect over Frame Relay* (obsoletes RFC 1490)
- RFC 2590, *Transmission of IPv6 Packets over Frame Relay Networks Specification*
- Internet draft draft-martini-frame-encap-mpls-01.txt, *Frame Relay Encapsulation over Pseudo-Wires* (expires December 2002)

Translation of the command/response bit and sequence numbers and padding are not supported.

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported GRE and IP-IP Interface Standards

Junos OS substantially supports the following RFCs, which define standards for generic routing encapsulation (GRE) and IP-IP interfaces.

- RFC 2003, *IP Encapsulation within IP*
- RFC 2784, *Generic Routing Encapsulation (GRE)*
- RFC 2890, *Key and Sequence Number Extensions to GRE*

The key field is supported, but the sequence number field is not.

The following RFCs do not define standards, but provide information about GRE, IP-IP, and related technologies. The IETF classifies them as “Informational.”

- RFC 1701, *Generic Routing Encapsulation (GRE)*

- RFC 1702, *Generic Routing Encapsulation over IPv4 networks*
- RFC 2547, *BGP/MPLS VPNs* (over GRE tunnels)

**Related  
Documentation**

- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported PPP Interface Standards

---

Junos OS substantially supports the following RFCs, which define standards for Point-to-Point Protocol (PPP) interfaces.

- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1334, *PPP Authentication Protocols*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*
- RFC 1989, *PPP Link Quality Monitoring*
- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2615, *PPP over SONET/SDH*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

The following features are not supported:

- Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
- Prefix elision
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

The following RFCs do not define standards, but provide information about PPP. The IETF classifies them as “Informational.”

- RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 2153, *PPP Vendor Extensions*

**Related  
Documentation**

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported SDH and SONET Interface Standards

Junos OS substantially supports the following standards for SDH and SONET interfaces.

- American National Standards Institute (ANSI) standard T1.105-2001, *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*
- ANSI standard T1.105.02-2001, *Synchronous Optical Network (SONET) – Payload Mappings*
- ANSI standard T1.105.06-2002, *Synchronous Optical Network (SONET): Physical Layer Specifications*
- GR-253-CORE (Telcordia Generic Requirements standard), *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* (replaces GR-1377-CORE, SONET OC-192 Transport System Generic Criteria)
- GR-499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*
- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.691, *Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers*
- ITU–T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.783 (1994), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*
- ITU–T Recommendation G.813 (1996), *Timing characteristics of SDH equipment slave clocks (SEC)*
- ITU–T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit-rate digital paths at or above the primary rate*
- ITU–T Recommendation G.831 (1993), *Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.957 (1995), *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*
- ITU–T Recommendation G.958 (1994), *Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables*
- ITU–T Recommendation I.432 (1993), *B-ISDN user-network interface – Physical layer specification*
- RFC 1619, *PPP over SONET/SDH*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Serial Interface Standards

---

Junos OS substantially supports the following standards for serial interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation V.35, *Data transmission at 48 kilobits per second using 60-108 kHz group band circuits*
- ITU–T Recommendation X.21 (1992), *Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported T3 Interface Standard

---

Junos OS substantially supports International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.703, *Physical/electrical characteristics of hierarchical digital interfaces*.

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

# Layer 2 Standards

- [Supported Layer 2 Networking Standards on page 2253](#)
- [Supported L2TP Standards on page 2254](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Supported Security Standards on page 2256](#)

## Supported Layer 2 Networking Standards

---

Junos OS substantially supports the following standards for Layer 2 networking.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ab, *IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery*
- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

This document includes the standard for Rapid Spanning Tree Protocol (RSTP), which is often referred to as 802.1w. It also discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.

### Related Documentation

- [Supported L2TP Standards on page 2254](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported L2TP Standards

---

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported VPWS Standards

---

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

Junos OS does not support Section 5.3, "The Generalized PWid FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as “Historic.”

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

Junos OS differs from the Internet draft in the following ways:

- A packet with a sequence number of 0 (zero) is treated as out of sequence.
- Any packet that does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

**Related Documentation**

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported Multicast VPN Standards on page 2296](#)
- [Supported VPLS Standards on page 2296](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported Layer 2 VPN Standards

Junos OS substantially supports the following Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvnp-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

**Related Documentation**

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported Multicast VPN Standards on page 2296](#)
- [Supported VPLS Standards on page 2296](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Security Standards

---

Junos OS substantially supports the following standard for security.

- IEEE Standard 802.1AE, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*

This document will facilitate standard secure communication between two security devices through secure chassis cluster control and fabric ports.

SRX340 and SRX345 supports only 802.1AE-2006 standard.

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)



# MPLS Applications Standards

- [Supported GMPLS Standards on page 2257](#)
- [Supported LDP Standards on page 2258](#)
- [Supported MPLS Standards on page 2259](#)
- [Supported RSVP Standards on page 2262](#)

## Supported GMPLS Standards

---

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for Generalized MPLS (GMPLS).

- RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

Only the following features are supported:

- Bidirectional LSPs (upstream label only)
  - Control channel separation
  - Generalized label (suggested label only)
  - Generalized label request (bandwidth encoding only)
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*  
Only Section 9, "Fault Handling," is supported.
  - RFC 4202, *Routing Extensions in Support of Generalized Multi-Protocol Label Switching*  
Only interface switching is supported.
  - RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
  - Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
  - Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control*

Only S,U,K,L,M-format labels and SONET traffic parameters are supported.

- Internet draft draft-ietf-ccamp-lmp-10.txt, *Link Management Protocol (LMP)*
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching*

The following sub-TLV types for the Link type, link, value (TLV) are not supported:

- Link Local/Remote Identifiers (type 11)
- Link Protection Type (type 14)
- Shared Risk Link Group (SRLG) (type 16)

The features described in Section 2 of the draft, “Implications on Graceful Restart,” are also not supported.

The Interface Switching Capability Descriptor (type 15) sub-TLV type is implemented, but only for packet switching.

- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

#### Related Documentation

- [Supported LDP Standards on page 2258](#)
- [Supported MPLS Standards on page 2259](#)
- [Supported RSVP Standards on page 2262](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported LDP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for LDP.

- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- Internet draft draft-napierala-mpls-targeted-mldp-01.txt, *Using LDP Multipoint Extensions on Targeted LDP Sessions*

The following RFCs do not define standards, but provide information about LDP. The IETF classifies them as “Informational.”

- RFC 3215, *LDP State Machine*
- RFC 5036, *LDP Specification*

For the following features described in the indicated sections of the RFC, Junos OS supports one of the possible modes but not the others:

- Label distribution control (section 2.6.1): Ordered mode is supported, but not Independent mode.

- Label retention (section 2.6.2): Liberal mode is supported, but not Conservative mode.
  - Label advertisement (section 2.6.3): Both Downstream Unsolicited mode and Downstream on Demand mode are supported.
  - RFC 5443, *LDP IGP Synchronization*
  - RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*
- Junos OS support limited to point-to-multipoint extensions for LDP.

#### Related Documentation

- [Supported GMPLS Standards on page 2257](#)
- [Supported MPLS Standards on page 2259](#)
- [Supported RSVP Standards on page 2262](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported MPLS Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for MPLS and traffic engineering.

- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3032, *MPLS Label Stack Encoding*
- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*  
Only E-LSPs are supported.
- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*  
Node protection in facility backup is not supported.
- RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*
- RFC 4385, *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*.

Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.

- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*
- RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*
- RFC 5317, *Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile*
- RFC 5586, *MPLS Generic Associated Channel*
- RFC 5654, *Requirements of an MPLS Transport Profile*

The following capabilities are supported in the Junos OS implementation of MPLS Transport Profile (MPLS-TP):

- MPLS-TP OAM can send and receive packets with GAL and G-Ach, without IP encapsulation.
  - Two unidirectional RSVP LSPs between a pair of routers can be associated with each other to create an associated bidirectional LSP for binding a path for the GAL and G-Ach OAM messages. A single Bidirectional Forwarding Detection (BFD) session is established for the associated bidirectional LSP.
  - RFC 5712, *MPLS Traffic Engineering Soft Preemption*
  - RFC 5718, *An In-Band Data Communication Network For the MPLS Transport Profile*
  - RFC 5860, *Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks*
  - RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*
  - RFC 5921, *A Framework for MPLS in Transport Networks*
  - RFC 5950, *Network Management Framework for MPLS-based Transport Networks*
  - RFC 5951, *Network Management Requirements for MPLS-based Transport Networks*
  - RFC 5960, *MPLS Transport Profile Data Plane Architecture*
  - RFC 6215, *MPLS Transport Profile User-to-Network and Network-to-Network Interfaces*
  - RFC 6291, *Guidelines for the Use of the "OAM" Acronym in the IETF.*
  - RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*
  - RFC 6371, *Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks.*
  - RFC 6372, *MPLS Transport Profile (MPLS-TP) Survivability Framework*
  - RFC 6373, *MPLS-TP Control Plane Framework*
  - RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*
- Only Point-to-Multipoint LSPs are supported.
- RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*

- RFC 6425, *Detecting Data-Plane Failures in Point-to-Multipoint MPLS – Extensions to LSP Ping*
- RFC 6426, *MPLS On-Demand Connectivity Verification and Route Tracing*
- RFC 6428, *Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile*
- Internet draft draft-ietf-mpls-rsvp-te-no-php-oob-mapping-01.txt, *Non PHP behavior and Out-of-Band Mapping for RSVP-TE LSPs*

The following RFCs and Internet drafts do not define standards, but provide information about MPLS, traffic engineering, and related technologies. The IETF classifies them variously as “Experimental,” “Historic,” or “Informational.”

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 2917, *A Core MPLS IP VPN Architecture*
- RFC 3063, *MPLS Loop Prevention Mechanism*
- RFC 3208, *PGM Reliable Transport Protocol Specification*
- RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

Junos OS differs from the Internet draft in the following ways:

- A packet with a sequence number of 0 is treated as out of sequence.
- Any packet that does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*
- Internet draft draft-raggarwa-mpls-p2mp-te-02.txt, *Establishing Point to Multipoint MPLS TE LSPs*

The features discussed in the indicated sections of the draft are not supported:

- Nonadjacent signaling for branch LSPs (section 7.1)

- Make-before-break and fast reroute (section 9)
- LSP hierarchy using point-to-point LSPs (section 10)

**Related  
Documentation**

- [Supported GMPLS Standards on page 2257](#)
- [Supported LDP Standards on page 2258](#)
- [Supported RSVP Standards on page 2262](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported RSVP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for RSVP.

- RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (updated by RFC 3097)
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication—Updated Message Type Value*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

The Null Service Object for maximum transmission unit (MTU) signaling in RSVP is not supported.

- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

Only Section 9, “Fault Handling,” is supported.

- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*  
(OSPF extensions can carry traffic engineering information over unnumbered links.)
- RFC 4558, *Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement*
- RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

The RRO node ID subobject is for use in inter-AS link and node protection configurations.

- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*

The following RFCs do not define standards, but provide information about RSVP and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2216, *Network Element Service Specification Template*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

**Related  
Documentation**

- [Supported GMPLS Standards on page 2257](#)
- [Supported LDP Standards on page 2258](#)
- [Supported MPLS Standards on page 2259](#)
- [Accessing Standards Documents on the Internet on page 2227](#)





# Open Standards

- [Supported Open Standards on page 2265](#)

## Supported Open Standards

---

Junos OS substantially supports the following open standards:

- *OpenFlow Switch Specification, Version 1.0.0*

For a detailed list of supported messages and fields, match conditions, wild cards, flow actions, statistics, and features, see *OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS*.

The Junos OS implementation of OpenFlow v1.0 differs from the specification in the following ways:

(The sections of the OpenFlow specification are indicated in the parentheses.)

- Junos OS supports only the following flow action types (section 5.2.4):
  - OFPAT\_OUTPUT—supports OFPP\_NORMAL, OFPP\_FLOOD, OFPP\_ALL, and OFPP\_CONTROLLER for normal flow actions, and OFPP\_FLOOD and OFPP\_ALL for Send Packet flow actions.
  - OFPAT\_SET\_VLAN\_VID—support varies by platform.
  - OFPAT\_STRIP\_VLAN—support varies by platform
- Flow priority is supported according to OpenFlow Switch Specification v1.3.0 in which there is no prioritization of exact match entries over wildcard entries.
- Emergency mode as defined in OpenFlow v1.0 is not supported. If the controller connection is lost and cannot be reestablished, the switch maintains all flow states in the control and data planes.

The following features are not supported:

- Encryption through TLS connection (section 4.4)
- 802.1D Spanning Tree Protocol (sections 4.5 and 5.2.1)
- OFPP\_LOCAL virtual port (section 5.2.1)
- Physical port features OFPPF\_PAUSE and OFPPF\_PAUSE\_ASYM (section 5.2.1)

- Queue structures and queue configuration messages (section 5.2.2 and 5.3.4)
- Flow action types: OFPAT\_SET\_VLAN\_PCP, OFPAT\_SET\_DL\_SRC/DST, OFPAT\_SET\_NW\_SRC/DST/TOS, OFPAT\_SET\_TP\_SRC/DST and OFPAT\_ENQUEUE (section 5.2.4)
- buffer\_id for Modify Flow Entry Message, Send Packet Message, and Packet-In Message (sections 5.3.3, 5.3.6, and 5.4.1)
- Port Modification Message (section 5.3.3)
- Vendor Statistics (section 5.3.5)
- Vendor message (section 5.5.4)

- *OpenFlow Switch Specification, Version 1.3.1*

For a detailed list of supported messages and fields, port structure flags and numbering, match conditions, flow actions, multipart messages, flow instructions, and group types, see *OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS*.

The Junos OS implementation of OpenFlow v1.3.1 differs from the specification in the following ways:

(The sections of the OpenFlow specification are indicated in the parentheses.)

- Junos OS supports only the following flow action types (section 5.12):
  - OFPAT\_SET\_VLAN\_VID
  - OFPAT\_POP\_VLAN
  - OFPAT\_GROUP
- Junos OS supports only the following group types (section 5.6.1):
  - OFPGT\_ALL
  - OFPGT\_INDIRECT
- Junos OS supports only one flow instruction per flow entry. Further, only the following flow instructions (section A.2.4) are supported:
  - OFPIT\_WRITE\_ACTIONS
  - OFPIT\_APPLY\_ACTIONS
- For OFPT\_SET\_CONFIG (section A.3.2), Junos OS supports only the OFPC\_FRAG\_NORMAL configuration flag, and the OFPCML\_NO\_BUFFER setting for the miss\_send\_len field.
- On MX Series routers, Junos OS supports only the following IPv6-related match conditions (A.2.3.7):
  - OFPXMT\_OFB\_IPV6\_SRC
  - OFPXMT\_OFB\_IPV6\_DST

The following features are not supported:

- Multiple flow tables (section 5)
- Table metadata (section 2)
- Action sets (section 5.10)
- Meter (section 5.7)
- MPLS fields (section 5.12.1)
- MPLS actions (section 5.10 and 5.12)
- Encryption through TLS connection (section 6.3.3)
- Per-port queues (section A.2.2)
- Auxiliary connections (section 6.3.5)
- Multiple virtual switches (section A.3.1)
- IPv6-related set-field actions (5.12)

**Related  
Documentation**

- *OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS*
- *OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS*
- *Understanding OpenFlow Operation and Forwarding Actions on Devices Running Junos OS*



# Packet Processing Standards

- [Supported CoS Standards on page 2269](#)
- [Supported Packet Filtering Standards on page 2270](#)
- [Supported Policing Standard on page 2270](#)

## Supported CoS Standards

---

Junos OS substantially supports the following standards for class of service (CoS).

- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

This document discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*

The following RFCs do not define standards, but provide information about CoS and related technologies. The IETF classifies them as “Informational.”

- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*
- RFC 2983, *Differentiated Services and Tunnels*
- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Packet Filtering Standards

---

Junos OS provides a packet filtering language that enables you to control the flow of packets being forwarded to a network destination, as well as packets destined for and sent by the router. It substantially supports the following RFCs, which define standards for packet filtering.

- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

The following RFCs do not define standards, but provide information about packet filtering and related technologies. The IETF classifies them as “Informational.”

- RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2983, *Differentiated Services and Tunnels*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

### Related Documentation

- *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Policing Standard

---

Junos OS supports policing, or rate limiting, to limit the amount of traffic that passes through an interface. For information about rate limiting, see RFC 2698, *A Two Rate Three Color Marker*.

The Junos OS implementation of policing uses a token-bucket algorithm and supports the following features:

- Adaptive shaping for Frame Relay traffic
- Virtual channels

- Related Documentation**
- [Accessing Standards Documents on the Internet on page 2227](#)





# Routing Protocol Standards

- [Supported Standards for BGP on page 2273](#)
- [Supported ES-IS Standards on page 2275](#)
- [Supported ICMP Router Discovery and IPv6 Neighbor Discovery Standards on page 2276](#)
- [Supported IP Multicast Protocol Standards on page 2276](#)
- [Supported IPv4, TCP, and UDP Standards on page 2278](#)
- [Supported IPv6 Standards on page 2280](#)
- [Supported Standards for IS-IS on page 2283](#)
- [Supported OSPF and OSPFv3 Standards on page 2284](#)
- [Supported RIP and RIPng Standards on page 2286](#)

## Supported Standards for BGP

---

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 4 (IPv4) BGP.

For a list of supported IP version 6 (IPv6) BGP standards, see [“Supported IPv6 Standards” on page 2280](#).

Junos OS BGP supports authentication for protocol exchanges (MD5 authentication).

- RFC 1745, *BGP4/IDRP for IP—OSPF Interaction*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1997, *BGP Communities Attribute*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2796, *BGP Route Reflection – An Alternative to Full Mesh IBGP*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 2918, *Route Refresh Capability for BGP-4*

- RFC 3065, *Autonomous System Confederations for BGP*
- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*
- RFC 3392, *Capabilities Advertisement with BGP-4*
- RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 4273, *Definitions of Managed Objects for BGP-4*
- RFC 4360, *BGP Extended Communities Attribute*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
- RFC 4486, *Subcodes for BGP Cease Notification Message*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*
- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*
- RFC 4724, *Graceful Restart Mechanism for BGP*
- RFC 4760, *Multiprotocol Extensions for BGP-4*
- RFC 4781, *Graceful Restart Mechanism for BGP with MPLS*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.

- RFC 4893, *BGP Support for Four-octet AS Number Space*
- RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*
- RFC 5065, *Autonomous System Confederations for BGP*
- RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*
- RFC 5291, *Outbound Route Filtering Capability for BGP-4 (partial support)*
- RFC 5292, *Address-Prefix-Based Outbound Route Filter for BGP-4 (partial support)*

Devices running Junos OS can receive prefix-based ORF messages.

- RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*
- RFC 5492, *Capabilities Advertisement with BGP-4*
- RFC 5575, *Dissemination of flow specification rules*
- RFC 5668, *4-Octet AS Specific BGP Extended Community*
- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

- RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*
- RFC 6811, *BGP Prefix Origin Validation*
- RFC 6996, *Autonomous System (AS) Reservation for Private Use*
- RFC 7300, *Reservation of Last Autonomous System (AS) Numbers*
- Internet draft draft-ietf-idr-add-paths-06.txt, *Advertisement of Multiple Paths in BGP* (expires March 2012)
- Internet draft draft-ietf-idr-aigp-06, *The Accumulated IGP Metric Attribute for BGP* (expires December 2011)
- Internet draft draft-ietf-idr-as0-06, *Codification of AS 0 processing* (expires February 2013)
- Internet draft draft-ietf-idr-link-bandwidth-01.txt, *BGP Link Bandwidth Extended Community* (expires August 2010)
- Internet draft draft-ietf-sidr-origin-validation-signaling-00, *BGP Prefix Origin Validation State Extended Community (partial support)* (expires May 2011)

The extended community (origin validation state) is supported in Junos OS routing policy. The specified change in the route selection procedure is not supported.

- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about BGP and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 1965, *Autonomous System Confederations for BGP*
- RFC 1966, *BGP Route Reflection—An alternative to full mesh IBGP*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (expires July 2002)

**Related  
Documentation**

- [Supported IPv6 Standards on page 2280](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported ES-IS Standards

Junos OS substantially supports the following standards for End System–to–Intermediate System (ES-IS).

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard 8473, *Information technology — Protocol for providing the connectionless-mode network service*

- ISO/IEC standard 9542, *Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*

**Related  
Documentation**

- [Supported Standards for IS-IS on page 2283](#)
- [IS-IS Overview](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported ICMP Router Discovery and IPv6 Neighbor Discovery Standards

Junos OS substantially supports the following RFCs, which define standards for the Internet Control Message Protocol (ICMP for IP version 4 [IPv4]) and neighbor discovery (for IP version 6 [IPv6]).

- RFC 1256, *ICMP Router Discovery Messages*
- RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4861, *IPv6 Stateless Address Autoconfiguration*
- RFC 4862, *Neighbor Discovery for IP version 6 (IPv6)*
- RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

**Related  
Documentation**

- [Supported IPv4, TCP, and UDP Standards on page 2278](#)
- [Supported IPv6 Standards on page 2280](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported IP Multicast Protocol Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP multicast protocols, including the Distance Vector Multicast Routing Protocol (DVMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multicast Source Discovery Protocol (MSDP), Pragmatic General Multicast (PGM), Protocol Independent Multicast (PIM), Session Announcement Protocol (SAP), and Session Description Protocol (SDP).

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*

- RFC 2327, *SDP: Session Description Protocol*
  - RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
  - RFC 2858, *Multiprotocol Extensions for BGP-4*
  - RFC 3031, *Multiprotocol Label Switching Architecture*
  - RFC 3376, *Internet Group Management Protocol, Version 3*
  - RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
  - RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
  - RFC 4601, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)*
  - RFC 4604, *Using IGMPv3 and MLDv2 for Source-Specific Multicast*
  - RFC 4607, *Source-Specific Multicast for IP*
  - RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*
  - RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
  - RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
- The scoping mechanism is not supported.
- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
  - RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
  - Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*
  - Internet draft draft-rosen-l3vpn-spmsi-joins-mldp-03.txt, *MVPN: S-PMSI Join Extensions for mLDP-Created Tunnels*

The following RFCs and Internet drafts do not define standards, but provide information about multicast protocols and related technologies. The IETF classifies them variously as “Best Current Practice,” “Experimental,” or “Informational.”

- RFC 1075, *Distance Vector Multicast Routing Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*
- RFC 2547, *BGP/MPLS VPNs*
- RFC 2974, *Session Announcement Protocol*
- RFC 3208, *PGM Reliable Transport Protocol Specification*
- RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
- RFC 3569, *An Overview of Source-Specific Multicast (SSM)*
- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

- RFC 3973, *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)*
  - RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
  - Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol*
  - Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8*
  - Internet draft draft-ietf-mmusic-sap-00.txt, *SAP: Session Announcement Protocol*
  - Internet draft draft-rosen-vpn-mcast-07.txt, *Multicast in MPLS/BGP VPNs*
- Only section 7, “Data MDT: Optimizing flooding,” is supported.

**Related  
Documentation**

- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported IPv4, TCP, and UDP Standards

Junos OS substantially supports the following RFCs, which define standards for IP version 4 (IPv4), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

- RFC 768, *User Datagram Protocol*
- RFC 791, *INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 793, *TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 826, *Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*
- RFC 854, *TELNET PROTOCOL SPECIFICATION*
- RFC 862, *Echo Protocol*
- RFC 863, *Discard Protocol*
- RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*
- RFC 896, *Congestion Control in IP/TCP Internetworks*
- RFC 903, *A Reverse Address Resolution Protocol*
- RFC 919, *BROADCASTING INTERNET DATAGRAMS*
- RFC 922, *BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*
- RFC 950, *Internet Standard Subnetting Procedure*
- RFC 959, *FILE TRANSFER PROTOCOL (FTP)*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*

- RFC 1042, *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1166, *INTERNET NUMBERS*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 2338, *Virtual Router Redundancy Protocol* (obsoleted by RFC 3768 in April 2004)
- RFC 2873, *TCP Processing of the IPv4 Precedence Field*
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

The following features are not supported:

- Row creation
- **Set** operation
- **vrrpv3StatisticsRowDiscontinuityTime** MIB object
- **vrrpv3StatisticsPacketLengthErrors** MIB object

The following RFCs do not define standards, but provide information about IP, TCP, UDP, and related technologies. The IETF classifies them as “Informational.”

- RFC 1878, *Variable Length Subnet Table For IPv4*
- RFC 1948, *Defending Against Sequence Number Attacks*

**Related  
Documentation**

- [Supported IPv6 Standards on page 2280](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported IPv6 Standards

---

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 6 (IPv6).

- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2375, *Multicast Address Assignments*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2472, *IP Version 6 over PPP*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2491, *IPv6 Over Non-Broadcast Multiple Access (NBMA) networks*
- RFC 2492, *IPv6 over ATM Networks*
- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2675, *IPv6 Jumbograms*
- RFC 2711, *IPv6 Router Alert Option*
- RFC 2740, *OSPF for IPv6* (partial support for RFC 5340)

Junos OS does not support the following components of RFC 5340:

- Multiple interfaces on the same link
- Deprecation of Multicast Extensions to OSPF (MOSPF) for IPv6
- Not-so-stubby area (NSSA) specification
- Link LSA suppression



- LSA options and prefix options updates
- IPv6 site-local addresses
- RFC 2784, *Generic Routing Encapsulation*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*
- RFC 2784, *Generic Routing Encapsulation*
- RFC 2878, *PPP Bridging Control Protocol (BCP)*
- RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*
- RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*
- RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

Address assignment is supported with IP version 4 (IPv4) but not IP version 6 (IPv6).

- RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*
- RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
- RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*
- RFC 3590, *Source Address Selection for the Multicast Listener D* (Supported for SSM include mode only)
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- RFC 3971, *Secure Neighbor Discovery for IPv6* (No support for certification paths, anchored on trusted parties)
- RFC 3972, *Cryptographically Generated Addresses*
- RFC 4087, *IP Tunnel MIB*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4292, *IP Forwarding Table MIB*
- RFC 4293, *Management Information Base for the Internet Protocol (IP)*
- RFC 4294, *IPv6 Node Requirements* (Partial support)
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.

- RFC 4861 *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*
- RFC 4942, *IPv6 Transition/Coexistence Security Considerations*
- RFC 5072, *IP Version 6 over PPP*
- RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*
- RFC 5308, *Routing IPv6 with IS-IS*
- RFC 5575, *Dissemination of Flow Specification Rules*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 5905, *Network Time Protocol Version 4 (for IPv6)*
- RFC 5952, *A Recommendation for IPv6 Address Text Representation*
- RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

The following features are not supported:

- Row creation
- **Set** operation
- **vrrpv3StatisticsPacketLengthErrors** MIB object
- **vrrpv3StatisticsRowDiscontinuityTime** MIB object
- RFC 6583, *Operational Neighbor Discovery Problems*

Only Tuning of the NDP Queue Rate Limit and Queue Tuning are supported.

- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP-MPLS IP VPN extension for IPv6 VPN*
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- Internet draft draft-ietf-softwire-dual-stack-lite-04.txt, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about IPv6 and related technologies. The IETF classifies them variously as "Experimental" or "Informational."

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*

- RFC 3587, *IPv6 Global Unicast Address Format*
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP*

Only MP-BGP over IP version 4 (IPv4) approach is supported.

**Related  
Documentation**

- [Supported IPv4, TCP, and UDP Standards on page 2278](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Standards for IS-IS

Junos OS substantially supports the following standards for IS-IS.

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO 9542, *End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for the Provision of the Connectionless-mode Network Service*
- ISO/IEC 10589, *Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3847, *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
- RFC 5120, *M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*
- RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*
- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 5302, *Domain-Wide Prefix Distribution with Two-Level IS-IS*
- RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*
- RFC 5304, *IS-IS Cryptographic Authentication*
- RFC 5305, *IS-IS Extensions for Traffic Engineering*
- RFC 5306, *Restart Signaling for IS-IS*
- RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*
- RFC 5308, *Routing IPv6 with IS-IS*

- RFC 5310, *IS-IS Generic Cryptographic Authentication*
- RFC 5880, *Bidirectional Forwarding Detection (BFD)*

The following RFCs do not define standards, but provide information about IS-IS and related technologies. The IETF classifies them as “Informational.”

- RFC 2973, *IS-IS Mesh Groups*
- RFC 3358, *Optional Checksums in Intermediate System to Intermediate System (ISIS)*
- RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*
- RFC 3373, *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*
- RFC 3567, *Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication*
- RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
- Internet draft draft-ietf-isis-wg-255adj-02.txt, *Maintaining more than 255 circuits in IS-IS*

**Related  
Documentation**

- *IS-IS Overview*
- [Supported ES-IS Standards on page 2275](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported OSPF and OSPFv3 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for OSPF and OSPF version 3 (OSPFv3).

- RFC 1583, *OSPF Version 2*
- RFC 1765, *OSPF Database Overflow*
- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 1850, *OSPF Version 2 Management Information Base*
- RFC 2154, *OSPF with Digital Signatures*
- RFC 2328, *OSPF Version 2*
- RFC 2370, *The OSPF Opaque LSA Option*

Support is provided by the **update-threshold** configuration statement at the **[edit protocols rsvp interface *interface-name* ]** hierarchy level.

- RFC 2740, *OSPF for IPv6* (partial support for RFC 5340)

Junos OS does not support the following components of RFC 5340:

- Multiple interfaces on the same link
- Deprecation of Multicast Extensions to OSPF (MOSPF) for IPv6
- Not-so-stubby area (NSSA) specification
- Link LSA suppression
- LSA options and prefix options updates
- IPv6 site-local addresses
- RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3623, *Graceful OSPF Restart*
- RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
- RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

Only interface switching is supported.

- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*
- RFC 4812, *OSPF Restart Signaling*
- RFC 4813, *OSPF Link-Local Signaling*
- RFC 4915, *Multi-Topology (MT) Routing in OSPF*
- RFC 5185, *OSPF Multi-Area Adjacency*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5250, *The OSPF Opaque LSA Option*



**NOTE:** RFC 4750, mentioned in this RFC as a "should" requirement is not supported. However, RFC 1850, the predecessor to RFC 4750 is supported.

- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5838, *Support of Address Families in OSPFv3*
- Internet draft draft-ietf-ospf-af-alt-10.txt, *Support of address families in OSPFv3*
- Internet draft draft-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection*

Transmission of echo packets is not supported.

The following RFCs do not define standards, but provide information about OSPF and related technologies. The IETF classifies them as “Informational.”

- RFC 3137, *OSPF Stub Router Advertisement*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

**Related  
Documentation**

- [Supported IPv6 Standards on page 2280](#)
- *OSPF Overview*
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported RIP and RIPng Standards

Junos OS substantially supports the following RFCs, which define standards for RIP (for IP version 4 [IPv4]) and RIP next generation (RIPng, for IP version 6 [IPv6]).

Junos OS supports authentication for all RIP protocol exchanges (MD5 or simple authentication).

- RFC 1058, *Routing Information Protocol*
- RFC 2080, *RIPng for IPv6*
- RFC 2082, *RIP-2 MD5 Authentication*

Multiple keys using distinct key IDs are not supported.

- RFC 2453, *RIP Version 2*

The following RFC does not define a standard, but provides information about RIPng. The IETF classifies it as “Informational.”

- RFC 2081, *RIPng Protocol Applicability Statement*

**Related  
Documentation**

- [Supported IPv4, TCP, and UDP Standards on page 2278](#)
- [Supported IPv6 Standards on page 2280](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

# Services PIC and DPC Standards

- Supported DTCP Standard on page 2287
- Supported Flow Monitoring and Discard Accounting Standards on page 2287
- Supported IPsec and IKE Standards on page 2288
- Supported L2TP Standards on page 2290
- Supported Link Services Standards on page 2290
- Supported NAT and SIP Standards on page 2291
- Supported RPM Standard on page 2291
- Supported Voice Services Standards on page 2292

## Supported DTCP Standard

---

Junos OS substantially supports Internet draft draft-cavuto-dtcp-03.txt, *DTCP: Dynamic Tasking Control Protocol*.

### Related Documentation

- Accessing Standards Documents on the Internet on page 2227

## Supported Flow Monitoring and Discard Accounting Standards

---

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions), Monitoring Services PICs, or Multiservices PICs or DPCs, Junos OS substantially supports the standards for cflowd version 5 and version 8 formats that are maintained by CAIDA and accessible at <http://www.caida.org>.

The following RFC does not define a standard, but provides information about flow monitoring. The IETF classifies it as “Informational.”

- RFC 3954, *Cisco Systems NetFlow Services Export Version 9*

On MX Series routers, Junos OS partially supports the following RFCs:

- RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*
- RFC 5102, *Information Model for IP Flow Information Export*

- Related Documentation**
- [Services Interfaces Overview for Routing Devices](#)
  - [MX Series Interface Module Reference](#)
  - [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported IPsec and IKE Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the Canada and U.S. version of Junos OS substantially supports the following RFCs, which define standards for IP Security (IPsec) and Internet Key Exchange (IKE).

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol* (obsoleted by RFC 4301)
- RFC 2402, *IP Authentication Header* (obsoleted by RFC 4302)  
This RFC is not supported on the ES PIC.
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH* (obsoleted by RFC 4305)
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)* (obsoleted by RFC 4303 and RFC 4305)
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP* (obsoleted by RFC 4306)
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)* (obsoleted by RFC 4306)
- RFC 2409, *The Internet Key Exchange (IKE)* (obsoleted by RFC 4306)
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2451, *The ESP CBC-Mode Cipher Algorithms*
- RFC 2460, *Internet Protocol, Version 6 (IPv6)*
- RFC 3193, *Securing L2TP using IPsec*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- RFC 3947, *Negotiation of NAT-Traversal in the IKE*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4301, *Security Architecture for the Internet Protocol*
- RFC 4302, *IP Authentication Header*  
This RFC is not supported on the ES PIC.
- RFC 4303, *IP Encapsulating Security Payload (ESP)*



- RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*



**NOTE:** Only Suite VPN-A is supported in Junos OS.

- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*

Junos OS partially supports the following RFCs for IPsec and IKE:

- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*
- RFC 5114, *Additional Diffie-Hellman Groups for Use with IETF Standards*
- RFC 5903, *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*

The following RFCs and Internet draft do not define standards, but provide information about IPsec, IKE, and related technologies. The IETF classifies them as “Informational.”

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- Internet draft draft-eastlake-sha2-02.txt, *US Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006)

#### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported L2TP Standards

---

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Link Services Standards

---

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFCs, which define standards for link services.

- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

The following features are not supported:

- Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
- Prefix elision

### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported NAT and SIP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following Network Address Translation (NAT) and Session Initiation Protocol (SIP) standards. NAT supports SIP dialogs and UDP/IP version 4 (IPv4) transport of SIP messages.

Junos OS substantially supports the following RFC and Internet draft.

- RFC 3261, *SIP: Session Initiation Protocol*
- Internet draft draft-mrw-behave-nat66-01.txt, *IPv6-to-IPv6 Network Address Translation (NAT66)*

The following RFCs do not define standards, but provide information about NAT. The IETF classifies them variously as “Best Current Practice,” “Historic,” or “Informational.”

- RFC 1631, *The IP Network Address Translator (NAT)*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 2766, *Network Address Translation - Protocol Translation (NAT-PT)*
- RFC 2993, *Architectural Implications of NAT*
- RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
- RFC 5382, *NAT Behavioral Requirements for TCP*
- RFC 5508, *NAT Behavioral Requirements for ICMP*

### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported RPM Standard

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports real-time performance monitoring (RPM), and provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

### Related Documentation

- [Services Interfaces Overview for Routing Devices](#)
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Voice Services Standards

---

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following following RFCs, which define standards for technologies used with voice services.

- RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
- RFC 2509, *IP Header Compression over PPP*

### Related Documentation

- *Services Interfaces Overview for Routing Devices*
- [MX Series Interface Module Reference](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

# VPLS and VPN Standards

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported EVPN Standards on page 2294](#)
- [Supported Layer 2 VPN Standards on page 2294](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported Multicast VPN Standards on page 2296](#)
- [Supported VPLS Standards on page 2296](#)

## Supported Carrier-of-Carriers and Interprovider VPN Standards

Junos OS substantially supports the following RFCs, which define standards for carrier-of-carriers and interprovider virtual private networks (VPNs).

- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*  
Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*  
Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 5601, *Pseudowire (PW) Management Information Base (MIB)*
- RFC 5603, *Ethernet Pseudowire (PW) Management Information Base (MIB)*
- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

### **Related Documentation**

- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported Multicast VPN Standards on page 2296](#)

- [Supported VPLS Standards on page 2296](#)
- [Supported Standards for BGP on page 2273](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported EVPN Standards

Junos OS supports the following RFCs and Internet drafts that define standards for EVPNs:

- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 7432, *BGP MPLS-Based Ethernet VPN*

The following features are not supported:

- Automatic derivation of Ethernet segment (ES) values. Only static ES configurations are supported.
- Host proxy ARP.
- MAC mobility extended community.
- VLAN bundle service interface.

### Related Documentation

- [EVPN Overview](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

---

## Supported Layer 2 VPN Standards

Junos OS substantially supports the following Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvnp-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported Multicast VPN Standards on page 2296](#)
- [Supported VPLS Standards on page 2296](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Layer 3 VPN Standards

Junos OS substantially supports the following RFCs, which define standards for Layer 3 virtual private networks (VPNs).

- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2685, *Virtual Private Networks Identifier*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

The traceroute functionality is supported only on transit routers.

- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

The following RFCs do not define a standard, but provide information about technology related to Layer 3 VPNs. The IETF classifies them as a “Best Current Practice” or “Informational.”

- RFC 1918, *Address Allocation for Private Internets*
- RFC 2917, *A Core MPLS IP VPN Architecture*

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Supported Multicast VPN Standards on page 2296](#)
- [Supported VPLS Standards on page 2296](#)
- [Supported MPLS Standards on page 2259](#)
- [Supported Standards for BGP on page 2273](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported Multicast VPN Standards

---

Junos OS substantially supports the following RFCs and Internet draft, which define standards for multicast virtual private networks (VPNs).

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN*
- RFC 6625, *Wildcards in Multicast VPN Auto-Discovery Routes*
- Internet draft draft-morin-l3vpn-mvpn-fast-failover-06.txt, *Multicast VPN Fast Upstream Failover*
- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
- [Supported VPWS Standards on page 2254](#)
- [Supported Layer 2 VPN Standards on page 2255](#)
- [Supported Layer 3 VPN Standards on page 2295](#)
- [Supported VPLS Standards on page 2296](#)
- [Supported MPLS Standards on page 2259](#)
- [Supported Standards for BGP on page 2273](#)
- [Accessing Standards Documents on the Internet on page 2227](#)

## Supported VPLS Standards

---

Junos OS substantially supports the following Internet RFCs and draft, which define standards for virtual private LAN service (VPLS).

- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
  - RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*
- FEC 128, FEC 129, control bit 0, the Ethernet pseudowire type 0x0005, and the Ethernet tagged mode pseudowire type 0x0004 are supported.
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
  - RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
  - Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*



- Related Documentation**
- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2293](#)
  - [Supported VPWS Standards on page 2254](#)
  - [Supported Layer 2 VPN Standards on page 2255](#)
  - [Supported Layer 3 VPN Standards on page 2295](#)
  - [Supported Multicast VPN Standards on page 2296](#)
  - [Accessing Standards Documents on the Internet on page 2227](#)



## PART 28

# Index

- [Index on page 2301](#)



# Index

## Symbols

|                                              |           |
|----------------------------------------------|-----------|
| !                                            |           |
| in interface names.....                      | 602       |
| " ", configuration group wildcards.....      | 622       |
| #, comments in configuration statements..... | lxiv, 492 |
| ( ), in syntax descriptions.....             | lxiv      |
| *                                            |           |
| in interface names.....                      | 601       |
| regular expression operator.....             | 602       |
| wildcard character.....                      | 622       |
| +                                            |           |
| in statement lists.....                      | 470       |
| regular expression operator.....             | 602       |
| . (period)                                   |           |
| regular expression operator.....             | 602       |
| /* */, comment delimiters.....               | 492       |
| /altconfig directory                         |           |
| altconfig file system.....                   | 322       |
| /altroot directory                           |           |
| altroot file system.....                     | 322       |
| /cf/var/crash directory See crash files      |           |
| /cf/var/log directory See system logs        |           |
| /cf/var/tmp directory See temporary files    |           |
| /config directory                            |           |
| config file system.....                      | 322       |
| /config/juniper.conf file.....               | 15        |
| /config/juniper.conf.1 file.....             | 15        |
| /config/rescue.conf file.....                | 15        |
| /etc/config/factory.conf file.....           | 15        |
| /var/log/mib2d file.....                     | 1585      |
| /var/log/snmpd file.....                     | 1585      |
| 64-bit                                       |           |
| Upgrade Routing Engine Junos OS.....         | 119       |
| < >, in syntax descriptions.....             | lxiv      |
| ?                                            |           |
| regular expression operator.....             | 622       |
| wildcard.....                                | 622       |
| [ ], in configuration statements.....        | lxiv      |

|                                       |      |
|---------------------------------------|------|
| \                                     |      |
| in interface names.....               | 601  |
| wildcard characters.....              | 622  |
| { }, in configuration statements..... | lxiv |
| specifying statements.....            | 541  |
| (pipe).....                           | 732  |
| command output.....                   | 732  |
| (pipe) command.....                   | 1397 |
| (pipe), in syntax descriptions.....   | lxiv |

|                                               |      |
|-----------------------------------------------|------|
| <b>A</b>                                      |      |
| AAA Objects MIB.....                          | 1427 |
| Access Authentication Objects MIB.....        | 1427 |
| access privilege levels                       |      |
| configuration example.....                    | 830  |
| configuration mode hierarchies.....           | 835  |
| operational mode commands.....                | 833  |
| configuring.....                              | 829  |
| configuration mode hierarchies.....           | 834  |
| operational mode commands.....                | 830  |
| entering configuration mode.....              | 462  |
| login classes.....                            | 799  |
| access privileges                             |      |
| denying and allowing commands.....            | 798  |
| permission bits for.....                      | 796  |
| predefined.....                               | 795  |
| specifying.....                               | 807  |
| access statement                              |      |
| usage guidelines.....                         | 1512 |
| access-list statement.....                    | 2044 |
| accounting options                            |      |
| configuration.....                            | 1678 |
| overview.....                                 | 1673 |
| accounting profiles                           |      |
| filter.....                                   | 1687 |
| interface.....                                | 1685 |
| MIB.....                                      | 1697 |
| Routing Engine.....                           | 1699 |
| accounting statement                          |      |
| authentication                                |      |
| usage guidelines.....                         | 1138 |
| accounting-options statement.....             | 1972 |
| accounts See template accounts; user accounts |      |
| action statement.....                         | 1246 |
| action-profile statement.....                 | 2006 |
| activate command.....                         | 660  |
| usage guidelines.....                         | 457  |
| activate statements and identifiers.....      | 489  |

|                                                 |               |
|-------------------------------------------------|---------------|
| activation                                      |               |
| of statements and identifiers in a Junos OS     |               |
| configuration.....                              | 490           |
| active                                          |               |
| configuration, logging .....                    | 194           |
| active configuration.....                       | 421, 423      |
| adaptive services interfaces                    |               |
| alarm conditions and configuration              |               |
| options.....                                    | 1705          |
| address                                         |               |
| command.....                                    | 199, 202      |
| statement.....                                  | 199, 202      |
| address statement                               |               |
| SNMPv3.....                                     | 2072          |
| usage guidelines.....                           | 1523          |
| Address-Assignment Pool                         |               |
| pool name.....                                  | 1095          |
| Address-Assignment Pools.....                   | 1094          |
| address-assignment pools                        |               |
| client attributes.....                          | 1115          |
| configuring overview.....                       | 1111          |
| DHCP attributes.....                            | 1115          |
| dhcpv6 attributes.....                          | 1115          |
| linking.....                                    | 1114          |
| named range.....                                | 1114          |
| router advertisement.....                       | 1116          |
| address-assignment statement.....               | 1196          |
| address-mask statement.....                     | 2073          |
| usage guidelines.....                           | 1523          |
| address-pool statement.....                     | 1199          |
| addresses                                       |               |
| configuring router.....                         | 198, 202      |
| default router.....                             | 199, 203      |
| hostname.....                                   | 198, 202      |
| IP.....                                         | 199, 203      |
| machine name.....                               | 198, 202, 432 |
| administrative roles                            |               |
| example.....                                    | 815           |
| AES encryption                                  |               |
| setting.....                                    | 1132          |
| agent-address statement.....                    | 2045          |
| alarm class See alarm severity                  |               |
| ALARM LED, color.....                           | 1703          |
| alarm management statement                      |               |
| edit snmp.....                                  | 2048          |
| Alarm MIB.....                                  | 1428          |
| alarm severity                                  |               |
| configuring for an interface.....               | 1709          |
| major (red) .....                               | 1704          |
| See also major alarms                           |               |
| minor (yellow).....                             | 1704          |
| See also minor alarms                           |               |
| alarm statement                                 |               |
| RMON.....                                       | 2020          |
| usage guidelines.....                           | 1627          |
| alarms.....                                     | 2174          |
| active, displaying at login.....                | 1709          |
| conditions, on an interface.....                | 1705          |
| configurable.....                               | 1705          |
| configuration requirements for interface        |               |
| alarms.....                                     | 1709          |
| licenses.....                                   | 1708          |
| major See major alarms                          |               |
| minor See minor alarms                          |               |
| overview.....                                   | 1703          |
| red See major alarms                            |               |
| rescue configuration.....                       | 1708          |
| severity See alarm severity                     |               |
| types.....                                      | 1703          |
| verifying.....                                  | 1711          |
| yellow See minor alarms                         |               |
| alarms, displaying                              |               |
| health monitor.....                             | 2191          |
| RMON.....                                       | 2203          |
| allow-commands statement                        |               |
| usage guidelines.....                           | 803           |
| allow-configuration statement.....              | 1200          |
| allow-configuration-regexps statement.....      | 1200          |
| usage guidelines.....                           | 803           |
| allowing commands to login classes.....         | 803           |
| altconfig, file system .....                    | 197, 207, 208 |
| altroot, file system .....                      | 197, 207, 208 |
| Analyzer MIB.....                               | 1428          |
| annotate command.....                           | 457, 661      |
| usage guidelines.....                           | 492           |
| ANSI standards supported See Index of Supported |               |
| Software Standards                              |               |
| Antivirus Objects MIB.....                      | 1428          |
| append command.....                             | 732           |
| apply-groups statement.....                     | 658           |
| usage guidelines.....                           | 617           |
| apply-groups-except statement.....              | 659           |
| archive-sites statement                         |               |
| accounting.....                                 | 1972          |
| usage guidelines.....                           | 1684          |

- 
- archiving files.....1302
  - arithmetic operators, for multicast traffic.....1946
  - AS path, displaying.....1821
  - AT commands, for modem initialization
    - description.....1037
  - ATM CoS MIB.....1428
  - ATM interfaces
    - supported software standards.....2247
  - ATM MIB.....1428
  - attacks
    - brute force, preventing.....1052
    - dictionary, preventing.....1052
  - authentication
    - local password, by default.....1022
    - login classes.....795, 807
    - methods.....798, 804
    - order of user authentication (configuration editor).....1022
    - RADIUS.....1011
    - RADIUS authentication (configuration editor).....1014
    - root password.....200, 204
    - specifying a method.....1022
    - specifying access privileges.....807
    - TACACS+.....1017
    - TACACS+ authentication (configuration editor).....1019
    - user accounts.....798, 807
  - authentication-key statement.....1201
  - authentication-md5 statement.....2073
    - usage guidelines.....1509
  - authentication-none statement.....2074
    - usage guidelines.....1510
  - authentication-order statement.....1202
  - authentication-password statement.....2075
    - usage guidelines.....1509
  - authentication-sha statement.....2076
    - usage guidelines.....1509
  - authorization See permissions
  - authorization statement.....2050
    - usage guidelines.....1479
  - auto-configuration.....274, 275
  - auto-image-upgrade statement.....277
  - auto-prefix delegation.....1124
  - auto-snapshot statement.....278
  - auto-snapshot, displaying the status of.....394
  - autoinstallation.....279
    - automatic configuration.....91
    - automatic configuration process.....83
    - CLI configuration editor.....84
    - default configuration file.....83, 90
    - establishing.....81
    - host-specific configuration file.....83, 90
    - interfaces.....82
    - IP address procurement process.....83
    - J-Web configuration editor.....84
    - overview.....81
    - protocols for procuring an IP address.....82
    - requirements.....84
    - router.....90
    - status.....86
    - TFTP server.....83, 90
    - verifying.....86
  - autoinstallation statement
    - for JNU satellites.....280
  - autoinstallation, compatibility with the DHCP server.....1092
  - autoinstallation, displaying the status of.....383
  - automatic configuration See autoinstallation
- B**
- backing up current installation
    - routers.....55
  - backing up partitions.....322
  - backup software, displaying information.....410
  - backups
    - copying to router.....202, 206
    - file systems .....197
    - software .....207
  - basic connectivity
    - requirements.....776
    - secure Web access.....1027
  - batch commit
    - usage guidelines.....516, 517
  - BFD MIB.....1428
  - BGP
    - supported software standards.....2273
  - BGP (Border Gateway Protocol)
    - monitoring.....1825
    - peers, probes to See BGP RPM probes
    - RPM probes to BGP neighbors See BGP RPM probes
    - statistics.....1825
  - BGP groups, displaying.....1825
  - BGP neighbors
    - directing RPM probes to.....1730
    - displaying.....1825
    - monitoring with RPM probes.....1728

|                                                   |                  |
|---------------------------------------------------|------------------|
| BGP peers See BGP neighbors                       |                  |
| BGP protocol                                      |                  |
| logging information.....                          | 195              |
| BGP routing information.....                      | 1825             |
| BGP RPM probes                                    |                  |
| directing to select BGP neighbors                 |                  |
| (configuration editor).....                       | 1730             |
| overview.....                                     | 1719             |
| setting up on local and remote device             |                  |
| (configuration editor).....                       | 1728             |
| BGP sessions, status.....                         | 1825             |
| BGP4 V2 MIB.....                                  | 1428             |
| binary operators, for multicast traffic.....      | 1946             |
| boot devices                                      |                  |
| alternative media.....                            | 36               |
| boot messages, displaying.....                    | 387              |
| boot sequence.....                                | 15               |
| M Series, MX Series, T Series, TX Matrix, TX      |                  |
| Matrix Plus, ACX Series, and PTX Series           |                  |
| routing engines.....                              | 34               |
| SRX Series devices.....                           | 36               |
| boot-server statement                             |                  |
| NTP.....                                          | 1203             |
| bootp.....                                        | 281              |
| BOOTP                                             |                  |
| supported software standards.....                 | 2232             |
| BOOTP, for autoinstallation.....                  | 84               |
| braces, in configuration statements.....          | lxiv             |
| brackets                                          |                  |
| angle, in syntax descriptions.....                | lxiv             |
| square, in configuration statements.....          | lxiv             |
| broadcast messages, synchronizing NTP.....        | 1205             |
| broadcast statement.....                          | 1204             |
| broadcast-client statement.....                   | 1205             |
| browser                                           |                  |
| downloading software.....                         | 49               |
| browser interface See J-Web interface             |                  |
| brute force attacks, preventing.....              | 1052             |
| built-in Ethernet ports See Ethernet ports;       |                  |
| management interfaces                             |                  |
| <b>C</b>                                          |                  |
| candidate configuration.....                      | 421, 423         |
| capture-file statement.....                       | 2007             |
| capturing packets See packet capture              |                  |
| categories statement.....                         | 2050             |
| usage guidelines.....                             | 1491             |
| category change software installation.....        | 41               |
| certificates See SSL certificates                 |                  |
| chassis                                           |                  |
| environment information, logging.....             | 191              |
| hardware                                          |                  |
| version, logging.....                             | 190              |
| monitoring.....                                   | 1850             |
| power management.....                             | 1850             |
| Chassis Cluster MIB.....                          | 1429             |
| chassis clusters                                  |                  |
| redundancy group IP address monitoring            |                  |
| configuration example.....                        | 1751             |
| Chassis Definitions for Router Model MIB.....     | 1428             |
| Chassis MIB.....                                  | 1429             |
| chassis software process.....                     | 17               |
| chassis-control                                   |                  |
| restart options.....                              | 218              |
| chassisd process.....                             | 17               |
| checklist for                                     |                  |
| reinstalling software .....                       | 187              |
| checksum                                          |                  |
| calculating for a file.....                       | 1304, 1305, 1306 |
| ciphers.....                                      | 1206             |
| Class 1 MIB objects.....                          | 1546             |
| Class 2 MIB objects.....                          | 1550             |
| Class 3 MIB objects.....                          | 1551             |
| Class 4 MIB objects.....                          | 1552             |
| Class-of-Service MIB.....                         | 1429             |
| class-usage-profile statement.....                | 1973             |
| usage guidelines.....                             | 1695             |
| cleaning up files.....                            | 1134, 1135       |
| cleanup, storage space.....                       | 364, 374         |
| clear                                             |                  |
| snmp history.....                                 | 2120             |
| clear chassis cluster ip-monitoring               |                  |
| failure-count.....                                | 2117             |
| clear chassis cluster ip-monitoring failure-count |                  |
| ip-address.....                                   | 2118             |
| clear dhcp client binding command.....            | 1291             |
| clear dhcp client statistics command.....         | 1292             |
| clear dhcp relay binding command.....             | 1293             |
| clear dhcp relay statistics command.....          | 1294             |
| clear dhcp server binding command.....            | 1295             |
| clear dhcp server statistics command.....         | 1296             |
| clear dhcpv6 server binding command.....          | 1299             |
| clear dhcpv6 server statistics command.....       | 1300             |
| clear ilmi statistics command.....                | 2119             |
| clear snmp history command.....                   | 2120             |
| clear snmp statistics command.....                | 2121             |
| clear system login lockout command.....           | 291, 1301        |



- 
- clear system services dhcp conflicts
    - command.....1089
  - CLI
    - breadcrumbs
      - usage guidelines.....654
    - command completion.....710
    - command history.....454
      - displaying.....725
    - comparing configuration versions.....526, 536
    - configuration mode
      - description.....456
      - navigation commands, table.....425
    - configuration-breadcrumbs statement.....668
    - current working directory
      - displaying.....724
      - setting.....711
    - date
      - setting.....719
    - editing command line.....599
    - idle timeout, setting.....712
    - keyboard sequences.....600
    - permissions, displaying.....723, 1345
    - prompt strings.....646
    - prompt, setting.....713
    - restart, after software upgrade.....714
    - screen length, setting.....715
    - screen width, setting.....716
    - settings, displaying.....720, 722
    - terminal type, setting.....717
    - timestamp.....646
    - timestamp, setting.....718
    - type checking.....543
    - users, monitoring.....571
    - word history.....454
    - working directory.....646
  - CLI configuration editor
    - autoinstallation.....84
    - controlling user access.....807
    - interface alarms.....1709
    - RADIUS authentication.....1014
    - RPM.....1721
    - secure access configuration.....1031
    - TACACS+ authentication.....1019
  - CLI users
    - monitoring.....468
  - client attributes
    - address-assignment pools.....1115
  - client list
    - adding to SNMP community.....1482
  - client-ia-type statement.....1208
  - client-identifier (dhcp-client) statement.....1208
  - client-identifier statement.....1209
  - client-list statement.....2051
    - usage guidelines.....1482
  - client-list-name statement.....1209, 2051
    - usage guidelines.....1482
  - client-type statement.....1210
  - clients statement.....2052
    - usage guidelines.....1479
  - cluster statement.....1998
  - command history
    - operational mode.....454
  - command output
    - configuration details.....499
    - configuration, comparing files.....590, 592
    - configuration, comparing files and displaying
      - in XML.....528
    - end of, displaying from.....594
    - filtering
      - comparing configuration
        - versions.....526, 536
    - JSON format, displaying.....593
    - number of lines, counting.....592
    - pagination, preventing.....595
    - regular expressions
      - first match, displaying from.....594
      - matching output, displaying.....595
      - nonmatching output, ignoring.....593
    - retaining.....594
    - RPC, displaying.....593
    - saving to a file.....596
    - sending to users.....595
    - XML format, displaying.....592
  - command shell.....421
  - command-line interface
    - downloading software.....49
  - commands
    - allowing or denying to login classes.....803
    - completion.....451, 647
    - configure.....647
    - filenames, specifying.....576
    - help about.....447
    - history.....454
    - options.....567
    - URLs, specifying.....576
  - commands for
    - reinstalling software .....187

|                                            |          |                                                 |               |
|--------------------------------------------|----------|-------------------------------------------------|---------------|
| comments                                   |          | compress-configuration-files statement          |               |
| adding to configuration file.....          | 492      | usage guidelines.....                           | 549           |
| comments, in configuration statements..... | lxiv     | compressing configuration files.....            | 549           |
| commit.....                                | 282      | compressing files.....                          | 1302          |
| persist-groups-inheritance.....            | 638      | config, file system.....                        | 197, 207, 208 |
| commit and-quit command                    |          | configuration                                   |               |
| usage guidelines.....                      | 510      | activating.....                                 | 534           |
| commit at command                          |          | adding comments.....                            | 492           |
| usage guidelines.....                      | 513      | autoinstallation of.....                        | 81            |
| commit command.....                        | 662      | candidate.....                                  | 421, 423      |
| usage guidelines.....                      | 457, 508 | committing.....                                 | 508, 783      |
| commit comment command                     |          | and exiting configuration mode.....             | 510           |
| usage guidelines.....                      | 515      | confirmation required.....                      | 512           |
| commit confirmed command                   |          | logging message about.....                      | 515           |
| usage guidelines.....                      | 512      | monitoring process.....                         | 514           |
| commit options                             |          | scheduling for later.....                       | 513           |
| J-Web.....                                 | 782      | synchronizing on Routing Engines.....           | 558           |
| commit scripts.....                        | 426      | comparing with previous.....                    | 526, 536      |
| commit synchronize command.....            | 662      | deleting                                        |               |
| commit synchronize statement               |          | statements.....                                 | 470           |
| usage guidelines.....                      | 560      | displaying                                      |               |
| commit   display detail command            |          | current configuration.....                      | 691           |
| usage guidelines.....                      | 514      | details.....                                    | 499           |
| commit-delay statement.....                | 2052     | downgrading software (CLI).....                 | 156           |
| usage guidelines.....                      | 1478     | downgrading software (J-Web).....               | 156           |
| commit-interval statement.....             | 667      | edit command, using.....                        | 469           |
| committing configuration                   |          | editing .....                                   | 779           |
| and exiting configuration mode.....        | 510      | files See configuration files                   |               |
| basic.....                                 | 508      | global replacement.....                         | 603           |
| confirmation required.....                 | 512      | installation on multiple devices.....           | 81            |
| logging message about.....                 | 515      | locking.....                                    | 467           |
| monitoring.....                            | 514      | merging current and new.....                    | 545           |
| scheduling for later.....                  | 513      | modifying.....                                  | 468           |
| synchronizing on Routing Engines.....      | 558      | previous, displaying.....                       | 535           |
| community statement                        |          | protecting.....                                 | 551           |
| RMON.....                                  | 2021     | replacing.....                                  | 544           |
| usage guidelines.....                      | 1630     | resource monitoring.....                        | 2031          |
| SNMP.....                                  | 2053     | saving to file.....                             | 539, 540      |
| usage guidelines.....                      | 1479     | storage of previous.....                        | 525           |
| community string, SNMP.....                | 1479     | unprotecting.....                               | 551           |
| community-name statement.....              | 2077     | upgrading (CLI).....                            | 150           |
| usage guidelines.....                      | 1537     | upgrading (J-Web).....                          | 65            |
| compare command.....                       | 732      | configuration example                           |               |
| usage guidelines.....                      | 526, 536 | activating and deactivating parts of a Junos OS |               |
| compare filter.....                        | 590, 592 | configuration.....                              | 490           |
| displaying in XML.....                     | 528      | configuration file                              |               |
| comparing files.....                       | 1307     | adding comments to.....                         | 494           |
| completing partial command entry.....      | 710      |                                                 |               |

- configuration files
  - compressing.....549
  - decrypting.....1131
  - encrypting.....1131
  - filename, specifying.....576
  - remote storage.....16
  - saving to files.....539, 540
  - sequence of selection.....15
  - URL, specifying.....576
- configuration groups
  - applying.....617
  - creating.....615
  - inheritance model.....614
  - inherited values.....620
  - interface parameters.....626, 628
  - nested groups.....617
  - overview.....614
  - peer entities.....630
  - re0, re1 groups.....615
  - regional configurations.....631
  - sets of statements.....625
  - wildcards.....622, 633
- Configuration Management MIB.....1429
- configuration mode, CLI.....470, 508
  - command completion.....451
  - commands
    - activate.....457
    - annotate.....457
    - commit.....457
    - copy.....457
    - deactivate.....457
    - delete.....457
    - edit.....457
    - exit.....457
    - extension.....457
    - help.....457
    - insert.....457
    - load.....457
    - paste.....458
    - quit.....458
    - rollback.....444, 458
    - run.....458
    - save.....458
    - set.....458
    - show.....458
    - status.....458
    - top.....458
    - up.....458
    - update.....458
  - configuration hierarchy, description.....460
  - description.....456
  - entering.....462, 468
  - example .....438
  - exiting.....463
  - global replacement.....603
  - identifier, description.....459
  - locking.....467
  - statement
    - container.....460
    - description.....459
    - leaf.....460
  - switching to operational mode.....431
  - top-level statements, interpreting.....459
  - users editing configuration
    - displaying.....504
    - multiple simultaneous users.....511
- configuration mode, entering.....728
- configuration statements
  - adding comments about.....492
  - deleting.....470
  - help about.....449
  - inheriting from groups.....625
  - overviews.....469
  - structure and components.....541
- configuration tasks
  - J-Web.....778
- configuration, router
  - active, logging .....194
  - backup, copying .....202, 206
- configuration-servers.....283
- configure command.....728
  - backup configurations, copying.....202, 206
  - names and addresses.....198, 202, 432
  - usage guidelines.....462, 564
- configure exclusive command
  - usage guidelines.....467
- configuring address-assignment pool
  - dhcpv6.....1111
- console port
  - disabling.....1051
  - securing.....1051
- contact statement.....2054
  - usage guidelines.....1474, 1476
- container hierarchy *See* hierarchy
- Content Filtering
  - verifying.....1858
- context (SNMPv3) statement .....2078
- controlling user access.....807

|                                                 |            |  |
|-------------------------------------------------|------------|--|
| conventions                                     |            |  |
| text and syntax.....                            | lxiii      |  |
| copy command.....                               | 473, 669   |  |
| example configuration.....                      | 476        |  |
| example of.....                                 | 473        |  |
| usage guidelines.....                           | 457, 564   |  |
| copying                                         |            |  |
| files.....                                      | 1310       |  |
| CoS                                             |            |  |
| measuring.....                                  | 1659       |  |
| MIB.....                                        | 1429       |  |
| supported software standards.....               | 2269       |  |
| CoS (class of service)                          |            |  |
| RPM probe classification.....                   | 1725       |  |
| <i>See also</i> TCP RPM probes; UDP RPM probes  |            |  |
| CoS components for link services                |            |  |
| applying on constituent links.....              | 1955       |  |
| count command.....                              | 732        |  |
| count filter.....                               | 592        |  |
| counters statement.....                         | 1974       |  |
| crash files                                     |            |  |
| cleaning up (CLI).....                          | 1135       |  |
| cleaning up (J-Web).....                        | 1134       |  |
| downloading (J-Web).....                        | 1137       |  |
| creating a new router configuration.....        | 173        |  |
| creating emergency boot device.....             | 165        |  |
| curly braces, in configuration statements.....  | lxiv       |  |
| current working directory                       |            |  |
| displaying.....                                 | 724        |  |
| setting.....                                    | 711        |  |
| cursor, moving.....                             | 600        |  |
| customer support.....                           | lxv        |  |
| contacting JTAC.....                            | lxv        |  |
| <b>D</b>                                        |            |  |
| daemons <i>See</i> processes, software          |            |  |
| data types, CLI.....                            | 543        |  |
| datapath-debug                                  |            |  |
| security.....                                   | 2008       |  |
| datapath-debug statement.....                   | 2008       |  |
| date                                            |            |  |
| setting from CLI.....                           | 719        |  |
| days-to-keep-error-logs statement.....          | 669        |  |
| deactivate command.....                         | 670        |  |
| usage guidelines.....                           | 457        |  |
| deactivate statements and identifiers           |            |  |
| usage guidelines.....                           | 489        |  |
| deactivation                                    |            |  |
| of statements and identifiers in a Junos OS     |            |  |
| configuration.....                              | 490        |  |
| decryption-failures statement.....              | 2041       |  |
| default configuration file, for                 |            |  |
| autoinstallation.....                           | 83, 90     |  |
| default configuration group.....                | 640        |  |
| delete command.....                             | 671        |  |
| usage guidelines.....                           | 457, 470   |  |
| delete-after-commit statement                   |            |  |
| for JNU satellites.....                         | 284        |  |
| deleting                                        |            |  |
| crash files (J-Web).....                        | 1134       |  |
| files.....                                      | 1312       |  |
| files, with caution.....                        | 1136       |  |
| licenses (CLI).....                             | 258, 1157  |  |
| licenses (J-Web).....                           | 1157       |  |
| log files (J-Web).....                          | 1134       |  |
| software packages.....                          | 347        |  |
| temporary files (J-Web).....                    | 1134       |  |
| deny-commands statement                         |            |  |
| usage guidelines.....                           | 803        |  |
| deny-configuration statement.....               | 1210       |  |
| deny-configuration-regexps statement            |            |  |
| usage guidelines.....                           | 803        |  |
| denying commands to login classes.....          | 803        |  |
| DES encryption                                  |            |  |
| setting.....                                    | 1132       |  |
| description statement                           |            |  |
| RMON.....                                       | 2021       |  |
| usage guidelines (alarms).....                  | 1627       |  |
| usage guidelines (events).....                  | 1630       |  |
| SNMP.....                                       | 2054       |  |
| usage guidelines.....                           | 1475, 1476 |  |
| Destination Class Usage MIB.....                | 1429       |  |
| destination statement.....                      | 1212       |  |
| usage guidelines.....                           | 1138       |  |
| destination-classes statement.....              | 1974       |  |
| usage guidelines.....                           | 1695       |  |
| destination-port statement                      |            |  |
| SNMP.....                                       | 2055       |  |
| usage guidelines.....                           | 1491       |  |
| device                                          |            |  |
| autoinstallation.....                           | 81         |  |
| multiple, deploying <i>See</i> autoinstallation |            |  |
| packet capture.....                             | 1928       |  |
| DHCP                                            |            |  |
| supported software standards.....               | 2232       |  |

- 
- DHCP (Dynamic Host Configuration Protocol)
    - autoinstallation, compatibility with.....1092
    - conflict detection and resolution.....1089
    - interface restrictions.....1090
    - options.....1091
    - overview.....1088
    - See also* DHCP leases; DHCP pages; DHCP pools; DHCP server
    - server function.....1088
  - DHCP Local Server
    - minimum configuration.....1093
  - DHCP MIB.....1429
  - DHCP server
    - preparation.....1092
    - sample configuration.....1092
  - dhcp-attributes statement IPv4.....1213
  - dhcp-attributes statement IPv6.....1215
  - dhcp-client attributes.....1101
  - dhcp-client statement.....1216
  - dhcp-local-server.....1217
  - DHCPv6
    - configure server options.....1109
  - dhcpv6.....1221
    - configuring address-assignment pool.....1111
  - DHCPv6 client
    - identification.....1116
    - minimum configuration.....1121
    - optional attributes.....1122
    - overview.....1120
    - TCP/IP propagation.....1126
  - DHCPv6 local server
    - overview.....1107
  - DHCPv6 MIB.....1429
  - dhcpv6 security policy configuration.....1108
  - DHCPv6 server
    - preparation.....1109
  - dhcpv6-client statement.....1224
  - diagnosis
    - alarm configurations.....1711
    - CLI command summary.....1399
    - displaying firewall filter for.....1937
    - displaying packet capture
      - configurations.....1932
    - interfaces.....1705, 1789
    - J-Web tools overview.....1398
    - license infringement.....1708
    - load balancing on the link services
      - interface.....1961
    - monitoring network performance.....1715
    - MPLS connections (J-Web).....1909
    - network traffic.....1943
    - packet capture.....1928
    - packet capture (J-Web).....1947
    - packet encapsulation on link services
      - interfaces.....1960
    - ping command.....1912
    - ping host (J-Web).....1914
    - ping MPLS (J-Web).....1909
    - ports.....1705
    - preparation.....1911
    - system operation.....1900
    - traceroute (J-Web).....1902
    - traffic analysis with packet capture.....1928
    - verifying captured packets.....1932
    - verifying dialer interfaces.....1045
    - verifying RPM probe servers.....1727
    - verifying RPM statistics.....1724
  - diagnostic commands.....1399
  - dial-in, USB modem
    - voice not supported.....1035
  - dial-up modem connection
    - connecting user end.....1049
  - dialer interface, for USB modem
    - adding (configuration editor).....1042
    - See also* USB modem connections
    - verifying.....1045
  - dialer interface, USB modem
    - limitations.....1035
    - naming convention.....1035
    - restrictions.....1035
  - dictionary attacks, preventing.....1052
  - DiffServ code points, bits for RPM probes.....1733
  - Digital Optical Monitoring MIB.....1430
  - directories
    - working, displaying.....724
  - disable statement
    - usage guidelines.....490
  - disabling
    - console port.....1051
    - packet capture.....1940
    - root login to console port.....1051
  - discard accounting
    - supported software standards.....2287
  - disconnection of console cable for console
    - logout.....1051
  - disk space, available
    - managing.....269
  - disk space, displaying .....197

|                                                 |          |
|-------------------------------------------------|----------|
| disk volume                                     |          |
| FreeBSD upgrade.....                            | 24       |
| display detail command                          |          |
| usage guidelines.....                           | 499      |
| display inheritance command                     |          |
| usage guidelines.....                           | 620      |
| display json filter.....                        | 593      |
| display set command                             |          |
| usage guidelines.....                           | 501      |
| display xml filter.....                         | 592, 593 |
| displaying                                      |          |
| licenses (J-Web).....                           | 1152     |
| dl0.....                                        | 1035     |
| dlv .....                                       | 1225     |
| DNS name resolution                             |          |
| troubleshooting.....                            | 1954     |
| DNS Objects MIB.....                            | 1430     |
| DNS server caching                              |          |
| configuring TTL value.....                      | 1072     |
| DNSSEC.....                                     | 1225     |
| secure domains configuring.....                 | 1074     |
| trusted keys configuring.....                   | 1074     |
| documentation                                   |          |
| comments on.....                                | lxv      |
| domain name, configuring.....                   | 199, 202 |
| downgrading                                     |          |
| software, with J-Web.....                       | 156      |
| software, with the CLI .....                    | 156      |
| download URL.....                               | 150      |
| downloading                                     |          |
| configuration, with autoinstallation.....       | 83       |
| crash files (J-Web).....                        | 1137     |
| licenses (J-Web).....                           | 1152     |
| log files (J-Web).....                          | 1137     |
| software upgrades.....                          | 150      |
| temporary files (J-Web).....                    | 1137     |
| downloading configuration, with                 |          |
| autoinstallation.....                           | 91       |
| downloading Junos OS.....                       | 48       |
| dropped traffic                                 |          |
| measuring.....                                  | 1662     |
| DS1 ports See T1 ports                          |          |
| DS3 ports See E3 ports; T3 ports                |          |
| DSCPs (DiffServ code points), bits for RPM      |          |
| probes.....                                     | 1733     |
| DTCP                                            |          |
| supported software standards.....               | 2287     |
| dual-root partitioning.....                     | 146      |
| dual-root partitioning scheme.....              | 105      |
| DVMRP                                           |          |
| supported software standards.....               | 2276     |
| Dynamic Flow Capture MIB.....                   | 1430     |
| Dynamic Host Configuration Protocol See DHCP    |          |
| <b>E</b>                                        |          |
| E3 ports, alarm conditions and configuration    |          |
| options.....                                    | 1705     |
| edit command.....                               | 672      |
| usage guidelines.....                           | 457      |
| editing command line.....                       | 599      |
| egress See RPM probes, outbound times           |          |
| Emacs keyboard sequences.....                   | 599      |
| emergency boot device                           |          |
| booting from.....                               | 36       |
| creating.....                                   | 165      |
| encapsulation overhead, PPP and MLPPP.....      | 1960     |
| encapsulation type                              |          |
| verifying for LFI and load balancing.....       | 1960     |
| encapsulation, modifying on packet              |          |
| capture-enabled interfaces.....                 | 1941     |
| encrypted access                                |          |
| through HTTPS.....                              | 1027     |
| through SSL.....                                | 1027     |
| encrypted passwords.....                        | 200, 204 |
| encrypted-password option.....                  | 200, 204 |
| engine-id statement                             |          |
| SNMPv3.....                                     | 2079     |
| usage guidelines.....                           | 1506     |
| enterprise-oid statement.....                   | 2055     |
| environment settings, CLI                       |          |
| command completion.....                         | 647      |
| displaying.....                                 | 647      |
| example configuration.....                      | 648      |
| idle timeout.....                               | 646      |
| prompt string.....                              | 646      |
| screen dimensions.....                          | 645, 647 |
| software upgrade, restarting after.....         | 646      |
| terminal type.....                              | 646      |
| timestamp.....                                  | 646      |
| working directory.....                          | 646      |
| environment, logging information .....          | 191      |
| erasing user data.....                          | 377      |
| ES-IS                                           |          |
| supported software standards.....               | 2275     |
| ESO Consortium standards supported See Index of |          |
| Supported Software Standards                    |          |
| Ethernet interface, configuring.....            | 199, 202 |

- 
- Ethernet interfaces
    - supported software standards.....2248
  - Ethernet MAC MIB.....1430
  - Ethernet ports
    - alarm conditions and configuration
      - options.....1705
    - autoinstallation on.....82
    - configuring alarms on.....1709
  - Event MIB.....1430
  - event statement.....2022
    - usage guidelines.....1630
  - event viewer, J-Web
    - overview.....1845
    - See also system log messages
  - events statement
    - usage guidelines.....1139
  - example
    - IP Monitoring.....1743
  - except command.....732
  - except filter.....593
  - exclude-cmd-attribute statement.....1271
  - exit command.....673
    - from configuration mode.....431
    - usage guidelines.....457, 463
  - exit configuration-mode command.....673
    - usage guidelines.....463
  - Experimental MIB.....1430
  - extension command
    - usage guidelines.....457
  - F**
  - falling-event-index statement.....2022
    - usage guidelines.....1627
  - falling-threshold statement
    - health monitor.....2015
    - usage guidelines.....1669
    - RMON.....2023
  - falling-threshold-interval statement
    - RMON.....2024
    - usage guidelines.....1628
  - family statement.....1226
  - fans, showing environmental information.....192
  - FAQ (frequently asked questions)
    - Are LFI and load balancing working correctly?.....1957
    - What causes jitter and latency on multilink bundles?.....1957
    - Which CoS components apply on link services interface?.....1955
  - feature licenses See licenses
  - fields statement
    - for interface profiles.....1975
    - usage guidelines.....1685
    - for Routing Engine profiles.....1976
    - usage guidelines.....1699
  - file archive command.....1302
  - file checksum md5 command.....1304
  - file checksum sha-256 command.....1306
  - file checksum sha1 command.....1305
  - file command.....730
    - usage guidelines.....564, 573
  - file compare command.....1307
  - file copy command.....202, 206, 1310
  - file delete command.....1312
  - file encryption
    - decrypting configuration files.....1132
    - encrypting configuration files.....1132
  - file list command.....1313
  - file management
    - configuration files.....1131
    - crash files (CLI).....1135
    - crash files (J-Web).....1134
    - log files.....1131
    - log files (CLI).....1135
    - log files (J-Web).....1134
    - packet capture file creation.....1929
    - temporary files (CLI).....1135
    - temporary files (J-Web).....1134
  - file rename command.....1314
  - file show command.....1315
  - file statement
    - accounting (associating with profile).....1977
    - usage guidelines (filter profile).....1688
    - usage guidelines (interface profile).....1685
    - usage guidelines (MIB profile).....1697
    - usage guidelines (Routing Engine profile).....1700
    - accounting (configuring log file).....1978
    - usage guidelines.....1682
  - file system
    - /altconfig.....197, 207, 208
    - /altroot .....197, 207, 208
    - backing up.....197
  - file systems
    - partitions, backing up.....322
  - filenames, specifying in commands.....576



|                                                |                  |
|------------------------------------------------|------------------|
| files                                          |                  |
| archiving.....                                 | 1302             |
| calculating checksum.....                      | 1304, 1305, 1306 |
| comparing.....                                 | 1307             |
| compressing.....                               | 1302             |
| configuration, compressing.....                | 549              |
| contents, displaying.....                      | 1315             |
| copying.....                                   | 1310             |
| deleting.....                                  | 1312             |
| list of, displaying.....                       | 1313             |
| listing.....                                   | 574              |
| renaming.....                                  | 1314             |
| saving command output to.....                  | 596              |
| saving configurations to files.....            | 539, 540         |
| viewing.....                                   | 573              |
| files statement.....                           | 1979             |
| filter profile.....                            | 1687             |
| filter-duplicates statement.....               | 2056             |
| usage guidelines.....                          | 1478             |
| filter-interfaces statement.....               | 2056             |
| filter-profile statement.....                  | 1980             |
| usage guidelines.....                          | 1687             |
| filtering                                      |                  |
| command output.....                            | 1397             |
| filtering get SNMP requests.....               | 1478             |
| finalizing software installation.....          | 63               |
| find command.....                              | 732              |
| find filter.....                               | 594              |
| FIPS See Junos-FIPS                            |                  |
| firewall filters                               |                  |
| for packet capture, configuring.....           | 1935             |
| for packet capture, overview.....              | 1929             |
| statistics                                     |                  |
| displaying.....                                | 1380             |
| Firewall MIB.....                              | 1430             |
| flags                                          |                  |
| login class.....                               | 799, 840         |
| user permissions.....                          | 799              |
| flash drive, internal.....                     | 197              |
| Flow Collection Services MIB.....              | 1430             |
| flow monitoring                                |                  |
| supported software standards.....              | 2287             |
| flow statement                                 |                  |
| (Security Flow).....                           | 2010             |
| font conventions.....                          | lxiii            |
| forwarding software process.....               | 17               |
| forwarding-options statement.....              | 1230             |
| fragmentation, verifying on the link services  |                  |
| interface.....                                 | 1959             |
| Frame Relay interfaces                         |                  |
| supported software standards.....              | 2249             |
| free-fw-memory-watermark statement             |                  |
| resource monitoring of memory blocks.....      | 2032             |
| free-heap-memory-watermark statement           |                  |
| resource monitoring of memory blocks.....      | 2033             |
| free-nh-memory-watermark statement             |                  |
| resource monitoring of memory blocks.....      | 2033             |
| FreeBSD                                        |                  |
| validate.....                                  | 361              |
| FreeBSD UNIX kernel.....                       | 422              |
| FreeBSD upgrade                                |                  |
| downgrading Junos OS.....                      | 209              |
| Junos OS.....                                  | 19               |
| Junos OS disk volumes.....                     | 24               |
| Junos OS package names.....                    | 22               |
| Junos OS snapshots.....                        | 23               |
| rebooting Junos OS.....                        | 316              |
| upgrading Junos OS.....                        | 139              |
| freeing up storage space.....                  | 364              |
| frequency, test See RPM probes, test intervals |                  |
| FRF (Broadband Forum) standards supported See  |                  |
| Index of Supported Software Standards          |                  |
| fwdd process.....                              | 17               |
| <b>G</b>                                       |                  |
| getting help                                   |                  |
| J-Web.....                                     | 765              |
| global-threshold statement.....                | 1999             |
| global-weight statement.....                   | 2000             |
| GMPLS                                          |                  |
| supported software standards.....              | 2257             |
| GR (Generic Requirements) standards supported  |                  |
| See Index of Supported Software Standards      |                  |
| GRE interfaces                                 |                  |
| supported software standards.....              | 2249             |
| group licenses.....                            | 1146             |
| group statement.....                           | 1231             |
| SNMPv3 (for access privileges).....            | 2081             |
| usage guidelines.....                          | 1518             |
| SNMPv3 (for configuring).....                  | 2080             |
| usage guidelines.....                          | 1513             |
| groups                                         |                  |
| BGP, displaying.....                           | 1825             |
| Groups Configuration Statement Hierarchy.....  | 1164             |
| groups statement.....                          | 674              |
| usage guidelines.....                          | 615              |



## H

- halting a switching platform
  - with J-Web .....219
- halting a switching platform immediately
  - with J-Web .....219
- hard disk.....30
- hardware
  - logging router chassis version .....190
  - major (red) alarm conditions on.....1704
  - timestamp See RPM probe timestamps
- hardware architecture
  - ACX Series, M Series, MX Series, T Series, and TX Matrix routers.....28
- health metrics of network.....1650
- health monitor alarms, displaying.....2191
- health-monitor statement.....2016
  - usage guidelines.....1669
- heat status, checking.....1850
- help apropos command
  - usage guidelines.....448
- help command.....676, 731
  - usage guidelines.....448, 457
- Help icon (?).....764
- help reference command
  - usage guidelines.....448
- help tip cli command
  - usage guidelines.....451
- high-threshold statement
  - resource monitoring of memory blocks.....2034
- history, CLI commands
  - displaying.....725
  - operational mode.....454
- hold command.....732
- hold filter.....594
- host reachability
  - ping command.....1912
  - ping host (J-Web).....1914
- Host Resources MIB.....1430
- host statement
  - ssh-known-hosts.....1234
- host-specific configuration file, for
  - autoinstallation.....83, 90
- hostkey-algorithm.....1235
- hostname
  - monitoring traffic by matching.....1945
  - opening an SSH session to.....1063
  - pinging (CLI).....1912
  - pinging (J-Web).....1914
  - resolving.....1092
  - telnetting to.....1062
  - tracing a route to (CLI).....1757, 1906
  - tracing a route to (J-Web).....1903
- hostname, logging.....190
- hostname.conf file, for autoinstallation.....83, 84, 90
- HTTP (Hypertext Transfer Protocol)
  - enabling Web access .....1029
  - enabling Web access (configuration editor).....1031
  - on built-in management interfaces.....1027
  - verifying configuration.....1032
- HTTP (Hypertext Transfer Protocol), RPM probes.....1716
- HTTPS (Hypertext Transfer Protocol over SSL)
  - enabling secure access.....1029
  - enabling secure access (configuration editor).....1031
  - J-Web configuration.....1029
  - recommended for secure access.....1027
  - verifying secure access configuration.....1032
- HTTPS Web access, establishing.....1027
- Hypertext Transfer Protocol See HTTP
- Hypertext Transfer Protocol over SSL See HTTPS
- Hypertext Transfer Protocol, RPM probes.....1716

## I

- IANA standards supported See Index of Supported Software Standards
- ICMP (Internet Control Message Protocol)
  - RPM probes, description.....1716
  - RPM probes, inbound and outbound times.....1717
  - RPM probes, setting.....1721
- ICMP router discovery
  - supported software standards.....2276
- icmp statement
  - RPM.....2012
- ICMPv6 (Internet Control Message Protocol)
  - RPM probes, setting.....1731
- identifiers
  - inserting in sequential lists.....481
  - renaming.....476
  - specifying.....541
- idle timeout
  - user, setting.....712
  - values, CLI sessions.....646
- IDP MIB.....1431
- idp potential violation statement.....2042

|                                                                                                                   |                  |
|-------------------------------------------------------------------------------------------------------------------|------------------|
| IEEE standards supported See Index of Supported Software Standards                                                |                  |
| ifd process.....                                                                                                  | 17               |
| IGMP                                                                                                              |                  |
| supported software standards.....                                                                                 | 2276             |
| ignore filter.....                                                                                                | 593              |
| IKE                                                                                                               |                  |
| supported software standards.....                                                                                 | 2288             |
| ILMI.....                                                                                                         | 1396             |
| statistics                                                                                                        |                  |
| clearing.....                                                                                                     | 2119             |
| displaying.....                                                                                                   | 2171             |
| inbound time See RPM probes                                                                                       |                  |
| INCITS standards supported See Index of Supported Software Standards                                              |                  |
| informs SNMP See SNMP informs                                                                                     |                  |
| ingress See RPM probes, inbound times                                                                             |                  |
| inheritance model, configuration groups.....                                                                      | 614              |
| inherited values, configuration groups.....                                                                       | 620              |
| init-command-string command.....                                                                                  | 1037             |
| insert command.....                                                                                               | 677              |
| usage guidelines.....                                                                                             | 457, 481         |
| Install Remote page                                                                                               |                  |
| field summary.....                                                                                                | 65, 110, 153     |
| installation                                                                                                      |                  |
| licenses (CLI).....                                                                                               | 257, 1154        |
| licenses (J-Web).....                                                                                             | 1154             |
| memory requirements                                                                                               |                  |
| M Series, MX Series, PTX Series, T Series, TX Matrix, and TX Matrix Plus routers.....                             | 29               |
| on router with redundant Routing Engines.....                                                                     | 58               |
| on router with single Routing Engine.....                                                                         | 57               |
| software upgrades (CLI).....                                                                                      | 150              |
| software upgrades, from a remote server.....                                                                      | 65, 152          |
| software upgrades, uploading.....                                                                                 | 65, 150          |
| installation bundles.....                                                                                         | 13               |
| installation media.....                                                                                           | 12               |
| installation modules.....                                                                                         | 14               |
| installation packages.....                                                                                        | 6                |
| installation types.....                                                                                           | 41               |
| installing software.....                                                                                          | 334, 335         |
| Instance to which this connection belongs                                                                         |                  |
| description.....                                                                                                  | 1910             |
| using.....                                                                                                        | 1917             |
| integrated local management interface See ILMI                                                                    |                  |
| interface                                                                                                         |                  |
| configuration example.....                                                                                        | 438              |
| Interface Accounting Forwarding Class MIB.....                                                                    | 1431             |
| Interface MIB.....                                                                                                | 1431             |
| interface name                                                                                                    |                  |
| replacing.....                                                                                                    | 606              |
| interface names                                                                                                   |                  |
| conventions.....                                                                                                  | 572              |
| interface profile.....                                                                                            | 1685             |
| interface software process.....                                                                                   | 17               |
| interface statement.....                                                                                          | 1236             |
| SNMP.....                                                                                                         | 2057             |
| usage guidelines.....                                                                                             | 1494             |
| interface-profile statement.....                                                                                  | 1981             |
| usage guidelines.....                                                                                             | 1685             |
| interface-traceoptions statement                                                                                  |                  |
| DHCP local server.....                                                                                            | 1239             |
| interfaces See management interfaces; network interfaces; ports                                                   |                  |
| media parameters.....                                                                                             | 626, 628         |
| router, logging .....                                                                                             | 194              |
| interfaces (ARP).....                                                                                             | 1237             |
| interfaces (autoinstallation).....                                                                                | 285              |
| interfaces limiting SNMP access.....                                                                              | 1494             |
| interfaces statement.....                                                                                         | 1238             |
| Internet draft                                                                                                    |                  |
| draft-ietf-mpls-rsvp-te-no-php-oob-mapping-01.txt, Non PHP behavior and Out-of-Band Mapping for RSVP-TE LSPs..... | 2261             |
| Internet draft                                                                                                    |                  |
| draft-kompella-l2vpn-vpls-multihoming-03.txt, Multi-homing in BGP-based Virtual Private LAN Service.....          | 2255, 2294, 2296 |
| Internet draft                                                                                                    |                  |
| draft-morin-l3vpn-mvpn-fast-failover-06.txt, Multicast VPN Fast Upstream Failover.....                            | 2296             |
| Internet draft                                                                                                    |                  |
| draft-napierala-mpls-targeted-mldp-01.txt, Using LDP Multipoint Extensions on Targeted LDP Sessions .....         | 2258             |
| Internet drafts supported See Index of Supported Software Standards                                               |                  |
| interval statement                                                                                                |                  |
| accounting.....                                                                                                   | 1982             |
| usage guidelines (filter profile).....                                                                            | 1689             |
| usage guidelines (interface profile).....                                                                         | 1686             |

- usage guidelines (MIB profile).....1698
  - usage guidelines (Routing Engine profile).....1700
  - health monitor.....2016
    - usage guidelines.....1669
  - RMON.....2024
    - usage guidelines.....1628
  - intervals, probe and test *See* RPM probes
  - IP Forward MIB.....1431
  - IP Monitoring.....1741, 1743
    - route failover.....1741
    - supported threshold.....1742
    - test parameter.....1742
  - IP multicast
    - supported software standards.....2276
  - IP-IP interfaces
    - supported software standards.....2249
  - ip-monitoring statement.....2001
  - IPsec
    - supported software standards.....2288
  - IPsec Generic Flow Monitoring Object MIB.....1431
  - IPsec Monitoring MIB.....1431
  - IPsec VPN Objects MIB.....1432
  - IPv4
    - supported software standards.....2278
  - IPv4 MIB.....1432
  - IPv6
    - supported software standards.....2280
  - IPv6 and ICMPv6 MIB.....1432
  - IPv6 SNMP community string.....1480
  - IS-IS
    - supported software standards.....2283
  - IS-IS protocol
    - logging information .....194
  - ISO/IEC standards supported *See* Index of Supported Software Standards
  - ISSU *See* unified in-service software upgrade
  - issuing relative configuration commands.....475
  - ITU-T Recommendations supported *See* Index of Supported Software Standards
- J**
- J-Web configuration
    - adding users.....807
    - authentication method.....1022
  - J-Web Configuration
    - secure Web access.....1029
  - J-Web configuration editor
    - autoinstallation.....84
    - controlling user access.....807
    - interface alarms.....1709
    - RADIUS authentication.....1014
    - RPM.....1721
    - secure access.....1031
    - TACACS+ authentication.....1019
  - J-Web graphical user interface (GUI).....426
  - J-Web interface
    - Diagnose options.....1398
    - event viewer.....1845
    - managing licenses.....1146
    - overview.....761
    - page layout.....762
    - starting.....762
  - J-Web software, installing.....769
  - jitter
    - description.....1717
      - See also* RPM probes
    - in RPM probes, improving with
      - timestamps.....1716
    - monitoring.....1736
    - threshold, setting.....1733
  - jitter, removing on multilink bundles.....1957
  - jnxRmonAlarmTable.....1622
  - JSON format
    - displaying command output in.....593
  - Juniper Networks MIB objects.....1542
  - juniper-ais configuration group
    - usage guidelines.....615
  - juniper.conf file, compressing.....549
  - Junos OS
    - auto-snapshot status, displaying.....394
    - autoinstallation.....81
    - autoinstallation status, displaying.....383
    - backing up .....207
    - boot messages, displaying.....387
    - checklist for
      - reinstalling .....187
    - configuration files.....15
    - downgrading from upgraded FreeBSD.....209
    - downloading.....48
    - editions.....5
      - Canada and U.S.....5
      - Junos-FIPS.....5
      - worldwide.....5
    - FreeBSD upgraded.....19
    - generating licenses.....1152

|                                        |         |                                                  |               |
|----------------------------------------|---------|--------------------------------------------------|---------------|
| information security.....              | 11      | Junos OS versions See Junos OS editions          |               |
| installation                           |         | JUNOS Software                                   |               |
| current configuration, confirming..... | 47      | bundles, deleting.....                           | 347           |
| PIC combinations, verifying.....       | 269     | packages, deleting.....                          | 347           |
| installation bundles.....              | 13      | rolling back.....                                | 351           |
| installation media.....                | 12      | upgrade                                          |               |
| installation modules.....              | 14      | performing.....                                  | 334           |
| installation packages.....             | 6       | validating candidate.....                        | 357           |
| introduction.....                      | 3       | Junos XML management protocol.....               | 426           |
| logging version.....                   | 189     | enabling secure access.....                      | 1029          |
| memory, resource utilization.....      | 2221    | verifying secure access configuration.....       | 1032          |
| naming convention.....                 | 9       | Junos XML protocol over SSL.....                 | 1029          |
| overview.....                          | 17      | junos-defaults configuration group.....          | 698           |
| packages                               |         | displaying.....                                  | 640, 694, 698 |
| digital signatures.....                | 11      | Junos-FIPS.....                                  | 5             |
| MD5 checksum.....                      | 11      | installation and configuration requirements..... | 6             |
| naming conventions.....                | 11      | password requirements.....                       | 6             |
| SHA-1 checksum.....                    | 11      | Junos-FIPS software environment.....             | 426           |
| Packet Forwarding Engine.....          | 17      | JUNOScript                                       |               |
| processes.....                         | 17      | enabling secure access.....                      | 772           |
| rebooting.....                         | 309     | <b>K</b>                                         |               |
| rebooting with FreeBSD upgrade.....    | 316     | kernel                                           |               |
| reconfiguring.....                     | 198     | downgrading from upgraded FreeBSD.....           | 209           |
| reinstalling.....                      | 36, 197 | FreeBSD upgrade.....                             | 19            |
| using emergency boot devices.....      | 172     | upgrading FreeBSD.....                           | 139           |
| using removable media.....             | 172     | key performance indicators.....                  | 1644          |
| release naming conventions.....        | 11      | keyboard sequences                               |               |
| release numbers.....                   | 11      | editing command line.....                        | 599           |
| Routing Engine.....                    | 17      | <b>L</b>                                         |               |
| software installation types.....       | 41      | L2ALD MIB.....                                   | 1432          |
| storage media.....                     | 30      | L2CP MIB.....                                    | 1432          |
| device names.....                      | 32, 34  | L2TP                                             |               |
| Upgrade Routing Engine to 64-bit.....  | 119     | supported software standards.....                | 2254, 2290    |
| upgrading.....                         | 146     | L2TP MIB.....                                    | 1432          |
| upgrading FreeBSD.....                 | 139     | label-switched paths See LSPs                    |               |
| version, displaying.....               | 48      | laptop See management device                     |               |
| Junos OS CLI                           |         | last command.....                                | 732           |
| access privilege levels.....           | 796     | last filter.....                                 | 594           |
| denying and allowing commands.....     | 798     | latency, in RPM probes, improving with           |               |
| diagnostic command summary.....        | 1399    | timestamps.....                                  | 1716          |
| filtering command output.....          | 1397    | latency, reducing on multilink bundles.....      | 1957          |
| Junos OS configuration                 |         | Layer 2 circuits                                 |               |
| adding comments to.....                | 494     | supported software standards.....                | 2254          |
| Junos OS disk volumes                  |         | Layer 2 circuits, monitoring.....                | 1909          |
| FreeBSD upgraded.....                  | 24      | Layer 2 Control Protocol                         |               |
| Junos OS package names                 |         | MIB.....                                         | 1432          |
| FreeBSD upgraded.....                  | 22      |                                                  |               |
| Junos OS snapshots                     |         |                                                  |               |
| FreeBSD upgraded.....                  | 23      |                                                  |               |

- Layer 2 networking
  - supported software standards.....2253
- Layer 2 VPNs, monitoring.....1909
- Layer 3 VPNs, monitoring.....1909
- layout, J-Web.....762
- LDP
  - MIB.....1432
  - supported software standards.....2258
- lease-time (dhcp-client) statement.....1242
- libpcap format, for packet capture files.....1932
- license infringement
  - identifying any licenses needed.....1146
  - verifying license usage.....261, 1156
  - verifying licenses installed.....260, 1156, 1158
- license keys
  - components.....225, 1145
  - displaying (CLI).....1156
  - status.....1146
  - version.....1146
- License MIB.....1433
- licenses.....225
  - adding.....302
  - adding (CLI).....257, 1154
  - adding (J-Web).....1154
  - deleting.....303
  - deleting (CLI).....258, 1157
  - deleting (J-Web).....1157
  - displaying.....398, 406, 1376
  - displaying (CLI).....260, 1156, 1158
  - displaying (J-Web).....1146, 1152
  - displaying usage.....261, 1156
  - downloading (J-Web).....1152
  - generating.....1152
  - group.....1146
  - infringement, preventing.....1146
    - See also license infringement
  - key.....1145
    - See also license keys
  - managing (J-Web).....1146
  - overview.....223, 1145
  - saving.....304
  - saving (CLI).....259, 1153
  - updating (CLI).....1154
  - verifying.....260, 1156, 1158
- licenses, alarm conditions and remedies.....1708
- limitations
  - ALARM LED lights yellow whether alarm is
    - minor or major.....1703
  - DHCP, no support on VPN interfaces.....1090
  - MPLS, no LSP statistics on outbound
    - device.....1797
  - mtrace from-source packet statistics always
    - O.....1759
  - performance degradation with monitor traffic
    - command.....1943
  - PPP, no J-Web monitoring information
    - available.....1800
  - Server relay and DHCP client cannot coexist in
    - device.....1088
  - software downgrade cannot be undone.....156
- link services
  - supported software standards.....2290
- link services interface
  - applying CoS components on constituent
    - links.....1955
  - fragmentation, troubleshooting.....1959
  - load balancing, troubleshooting.....1961
  - MLPPP header overhead.....1960
  - packet encapsulation, troubleshooting.....1960
  - PPP header overhead.....1960
  - preventing dropped packets on PVCs.....1964
  - reducing jitter and latency on multilink
    - bundles.....1957
  - troubleshooting LFI and load balancing.....1957
- load balancing on link services interfaces
  - FAQ.....1957
  - troubleshooting.....1957
  - verifying.....1961
- load command.....345, 346, 678
  - usage guidelines.....457
- load merge command.....202, 206
  - usage guidelines.....545
- load override command
  - usage guidelines.....544
- load replace command.....202, 206
- load set command
  - usage guidelines.....546
- local password
  - default authentication method for
    - system.....1022
  - method for user authentication .....1022
  - order of user authentication (configuration
    - editor).....1022
  - overview.....798, 804
- local template accounts.....810
- local-engine statement.....2083

|                                               |                      |
|-----------------------------------------------|----------------------|
| Locate LSP from interface name                |                      |
| description.....                              | 1910                 |
| using.....                                    | 1917                 |
| Locate LSP from virtual circuit information   |                      |
| description.....                              | 1910                 |
| using.....                                    | 1917                 |
| Locate LSP using interface name               |                      |
| description.....                              | 1910                 |
| using.....                                    | 1917                 |
| location statement                            |                      |
| SNMP.....                                     | 2057                 |
| usage guidelines.....                         | 1475, 1476           |
| locking configuration.....                    | 467                  |
| lockout-period statement.....                 | 1244                 |
| log files                                     |                      |
| archiving.....                                | 1131                 |
| deleting unused files.....                    | 1131                 |
| rotating.....                                 | 1131                 |
| logical interfaces                            |                      |
| summary information.....                      | 195                  |
| unit numbers.....                             | 572                  |
| logical operators, for multicast traffic..... | 1946                 |
| Logical Systems MIB.....                      | 1433                 |
| logical-system statement.....                 | 2058                 |
| logical-system-trap-filter statement.....     | 2059                 |
| login classes                                 |                      |
| access privilege levels.....                  | 799                  |
| commands, allowing or denying.....            | 803                  |
| defining (configuration editor).....          | 807                  |
| permission bits for.....                      | 796                  |
| predefined permissions.....                   | 795                  |
| specifying.....                               | 807                  |
| login lockout.....                            | 291, 409, 1301, 1379 |
| login retry limits, setting.....              | 1052                 |
| LSPs (label-switched paths)                   |                      |
| information about.....                        | 1796                 |
| monitoring, with ping MPLS.....               | 1909                 |
| statistics.....                               | 1798                 |
| LSYS MIB.....                                 | 1433                 |
| <b>M</b>                                      |                      |
| macs.....                                     | 1245                 |
| major (red) alarms                            |                      |
| description.....                              | 1704                 |
| management device                             |                      |
| diagnosing problems from.....                 | 1398                 |
| monitoring from.....                          | 1397                 |
| recovering root password from.....            | 1953                 |
| management interfaces                         |                      |
| alarm conditions and configuration            |                      |
| options.....                                  | 1705                 |
| configuring alarms on.....                    | 1709                 |
| monitoring.....                               | 1789, 1794           |
| statistics.....                               | 1789                 |
| management software process.....              | 17                   |
| managing                                      |                      |
| files.....                                    | 1131                 |
| reboots.....                                  | 219                  |
| software.....                                 | 146                  |
| user authentication.....                      | 804                  |
| manuals                                       |                      |
| comments on.....                              | lxv                  |
| match command.....                            | 732                  |
| match conditions, for multicast traffic       |                      |
| .....                                         | 1945                 |
| match filter.....                             | 595                  |
| maximum-aggregate-pool statement.....         | 679                  |
| maximum-capture-size                          |                      |
| security log.....                             | 2012                 |
| maximum-entries statement.....                | 680                  |
| MD5 (Message Digest 5) checksum.....          | 11                   |
| MD5 checksum, calculating.....                | 1304                 |
| measurement tests                             |                      |
| proxy ping.....                               | 1647                 |
| memory requirements                           |                      |
| M Series, MX Series, PTX Series, T Series, TX |                      |
| Matrix, and TX Matrix Plus routers.....       | 29                   |
| memory resource monitoring                    |                      |
| of regions or memory blocks on Packet         |                      |
| Forwarding Engine of an FPC.....              | 2221                 |
| message-processing-model statement.....       | 2084                 |
| usage guidelines.....                         | 1527                 |
| messages                                      |                      |
| boot, displaying.....                         | 387                  |
| broadcast messages, NTP.....                  | 1205                 |
| mgd process.....                              | 17                   |
| MIB object classes.....                       | 1552                 |
| MIB profile.....                              | 1697                 |
| mib-profile statement.....                    | 1983                 |
| usage guidelines.....                         | 1697                 |
| MIBs                                          |                      |
| AAA Objects.....                              | 1427                 |
| Access Authentication Objects.....            | 1427                 |
| Alarm.....                                    | 1428                 |
| Analyzer.....                                 | 1428                 |
| Antivirus Objects.....                        | 1428                 |
| ATM.....                                      | 1428                 |

|                                                            |            |
|------------------------------------------------------------|------------|
| ATM CoS.....                                               | 1428       |
| BFD.....                                                   | 1428       |
| BGP4 V2.....                                               | 1428       |
| Chassis.....                                               | 1429       |
| Chassis Cluster.....                                       | 1429       |
| Chassis Definitions for Router Model.....                  | 1428       |
| Class-of-Service.....                                      | 1429       |
| Configuration Management.....                              | 1429       |
| Destination Class Usage.....                               | 1429       |
| DHCP .....                                                 | 1429       |
| DHCPv6 .....                                               | 1429       |
| Digital Optical Monitoring.....                            | 1430       |
| DNS Objects.....                                           | 1430       |
| Dynamic Flow Capture.....                                  | 1430       |
| Ethernet MAC.....                                          | 1430       |
| Event.....                                                 | 1430       |
| EX Series                                                  |            |
| Analyzer.....                                              | 1428       |
| PAE Extension.....                                         | 1434       |
| Structure of Management Information .....                  | 1437       |
| Virtual Chassis.....                                       | 1438       |
| VLAN.....                                                  | 1438       |
| Experimental.....                                          | 1430       |
| Firewall.....                                              | 1430       |
| Flow Collection Services.....                              | 1430       |
| Host Resources.....                                        | 1430       |
| IDP.....                                                   | 1431       |
| Interface.....                                             | 1431       |
| IP Forward.....                                            | 1431       |
| IPsec Generic Flow Monitoring Object .....                 | 1431       |
| IPsec Monitoring.....                                      | 1431       |
| IPsec VPN Objects.....                                     | 1432       |
| IPv4.....                                                  | 1432       |
| IPv6 and ICMPv6.....                                       | 1432       |
| L2ALD.....                                                 | 1432       |
| L2CP .....                                                 | 1432       |
| L2TP.....                                                  | 1432       |
| Layer 2 Control Protocol.....                              | 1432       |
| LDP.....                                                   | 1432       |
| License.....                                               | 1433       |
| Logical Systems.....                                       | 1433       |
| LSYS.....                                                  | 1433       |
| MIMSTP.....                                                | 1433       |
| MPLS.....                                                  | 1433       |
| MPLS LDP.....                                              | 1433       |
| Multicast.....                                             | 1417, 1427 |
| MVPN.....                                                  | 1433       |
| NAT Objects.....                                           | 1434       |
| NAT Resources-Monitoring.....                              | 1434       |
| Optical Transport Network (OTN) Interface Management ..... | 1434       |
| OSPF.....                                                  | 1413       |
| Packet Forwarding Engine.....                              | 1434       |
| Packet Mirror.....                                         | 1434       |
| PAE Extension.....                                         | 1434       |
| Passive Monitoring.....                                    | 1434       |
| Ping.....                                                  | 1435       |
| use in ping test.....                                      | 1562       |
| view configuration example, SNMP.....                      | 1497       |
| Policy Objects.....                                        | 1435       |
| Power Supply Unit.....                                     | 1435       |
| PPP.....                                                   | 1413, 1435 |
| PPPoE.....                                                 | 1435       |
| Pseudowire ATM.....                                        | 1435       |
| Pseudowire TDM.....                                        | 1435       |
| PTP.....                                                   | 1436       |
| QoS Interface.....                                         | 1431       |
| Real-Time Performance Monitoring.....                      | 1436       |
| Reverse-Path-Forwarding.....                               | 1436       |
| RMON Events and Alarms .....                               | 1436       |
| RPM.....                                                   | 1436       |
| RSVP .....                                                 | 1436       |
| Security Interface Extension Objects.....                  | 1436       |
| Security Screening Objects.....                            | 1437       |
| Services PIC.....                                          | 1437       |
| SNMP IDP.....                                              | 1431       |
| SNMP object values, displaying.....                        | 2200       |
| SONET APS.....                                             | 1437       |
| SONET/SDH Interface Management.....                        | 1437       |
| Source Class Usage.....                                    | 1437       |
| SPU Monitoring.....                                        | 1437       |
| Structure of Management Information.....                   | 1437       |
| Junos OS for and SRX Series devices, for.....              | 1437       |
| Subscriber.....                                            | 1438       |
| System Log.....                                            | 1438       |
| Timing Feature Defect and Event Notification MIB.....      | 1436       |
| Traceroute.....                                            | 1438       |
| Utility.....                                               | 1438       |
| views                                                      |            |
| SNMP.....                                                  | 1496       |
| Virtual Chassis.....                                       | 1438       |
| VLAN.....                                                  | 1438       |

|                                               |                              |                                                 |            |
|-----------------------------------------------|------------------------------|-------------------------------------------------|------------|
| VPLS .....                                    | 1438                         | PPP (CLI).....                                  | 1800       |
| BGP MIB.....                                  | 1438                         | PPPoE.....                                      | 1801       |
| Generic MIB.....                              | 1438                         | preparation.....                                | 1911       |
| LDP MIB.....                                  | 1438                         | RIP.....                                        | 1822       |
| VPN.....                                      | 1439                         | routing information.....                        | 1820       |
| VPN Certificate Objects.....                  | 1439                         | routing tables.....                             | 1820       |
| MIMSTP                                        |                              | RPM probes.....                                 | 1736       |
| MIB.....                                      | 1433                         | service quality.....                            | 1643       |
| minimum accounting options configuration..... | 1680                         | system logs.....                                | 1900       |
| minor (yellow) alarms                         |                              | trace files.....                                | 1900       |
| description.....                              | 1704                         | monitoring the wx interface.....                | 1806       |
| MLD                                           |                              | MPLS                                            |            |
| supported software standards.....             | 2276                         | MIB.....                                        | 1433       |
| MLPPP encapsulation, on the link services     |                              | supported software standards.....               | 2259       |
| interface.....                                | 1960                         | MPLS (Multiprotocol Label Switching)            |            |
| Mobile IP                                     |                              | connections, checking.....                      | 1909       |
| supported software standards.....             | 2233                         | LSPs.....                                       | 1796       |
| model, logging router .....                   | 190                          | monitoring interfaces.....                      | 1796       |
| modem connection to router USB port           |                              | monitoring LSP information.....                 | 1796       |
| connecting USB modem to router.....           | 1038                         | monitoring LSP statistics.....                  | 1797, 1798 |
| monitor interface command.....                | 1789                         | monitoring MPLS interfaces.....                 | 1796       |
| controlling output.....                       | 1789                         | monitoring RSVP interfaces.....                 | 1799       |
| monitor interface traffic command.....        | 1789                         | monitoring RSVP sessions.....                   | 1798       |
| controlling output.....                       | 1790                         | monitoring traffic engineering.....             | 1795       |
| monitor list command.....                     | 1900                         | MPLS LDP MIB.....                               | 1433       |
| monitor start command.....                    | 1900                         | MPLS protocol, logging information.....         | 195        |
| monitor stop command.....                     | 1900                         | mpls statement.....                             | 1984       |
| monitor traffic command.....                  | 1943                         | MSDP                                            |            |
| options.....                                  | 1943                         | supported software standards.....               | 2276       |
| performance impact.....                       | 1943                         | mtrace monitor command.....                     | 1901       |
| monitor traffic matching command.....         | 1943                         | results.....                                    | 1902       |
| arithmetic, binary, and relational            |                              | mtrace-from-source command.....                 | 1759       |
| operators.....                                | 1946                         | options.....                                    | 1759       |
| logical operators.....                        | 1946                         | results.....                                    | 1761       |
| match conditions.....                         | 1945                         | multicast                                       |            |
| monitoring                                    |                              | trace operations, displaying.....               | 1901       |
| BGP.....                                      | 1825                         | tracing paths.....                              | 1759       |
| BGP neighbors, with RPM probes.....           | 1728                         | Multicast MIB.....                              | 1417, 1427 |
| chassis.....                                  | 1850                         | multicast-client statement.....                 | 1246       |
| interfaces.....                               | 1789, 1794                   | multilink bundles                               |            |
| Layer 2 circuits.....                         | 1909                         | preventing dropped packets.....                 | 1964       |
| Layer 2 VPNs.....                             | 1909                         | reducing latency.....                           | 1957       |
| Layer 3 VPNs.....                             | 1909                         | removing jitter.....                            | 1957       |
| MPLS traffic                                  |                              | multiple devices                                |            |
| engineering.....                              | 1795, 1796, 1797, 1798, 1799 | deploying See autoinstallation                  |            |
| network interface traffic.....                | 1943                         | Multiprotocol Label Switching See MPLS See MPLS |            |
| network traffic with packet capture.....      | 1928                         | MVPN MIB.....                                   | 1433       |
| OSPF.....                                     | 1824                         |                                                 |            |
| ports.....                                    | 1794                         |                                                 |            |



**N**

- name
    - configuring domain .....198, 202
    - configuring machine.....198, 202
  - name statement.....2059
    - usage guidelines.....1477
  - names
    - wildcard .....633
  - naming conventions, interface.....572
  - naming conventions, software.....9
  - NAT
    - supported software standards.....2291
  - NAT Objects MIB.....1434
  - NAT Resources-Monitoring MIB.....1434
  - neighbor discovery
    - supported software standards.....2276
  - neighbor-discovery-router-advertisement
    - statement.....1247
  - neighbors, BGP See BGP neighbors; BGP RPM
  - probes
  - nested configuration groups.....617
  - network
    - connectivity, checking .....201, 206
    - ping command.....201, 206
  - Network Address Translation Objects MIB See NAT Objects MIB
  - network health
    - measuring.....1650
  - network interfaces
    - alarm conditions and configuration
      - options.....1705
    - configuring alarms on.....1709
    - integrated services, alarm conditions and
      - configuration options.....1705
    - monitoring.....1789, 1794
    - monitoring MPLS traffic engineering.....1796
    - monitoring traffic.....1943
    - monitoring, PPPoE.....1801
    - monitoring, RSVP.....1799
    - packet capture, configuring on.....1933
    - packet capture, disabling before changing
      - encapsulation.....1941
    - packet capture, supported on.....1928
    - services, alarm conditions and configuration
      - options.....1705
    - statistics.....1789
  - network management
    - supported software standards.....2233
  - network performance See RPM
    - measuring.....1656
  - network.conf file, default for
    - autoinstallation.....83, 84, 90
  - new identifier
    - inserting, example of.....481
  - next hop, displaying.....1821
  - no-cmd-attribute-value statement.....1271
  - no-compress-configuration-files statement
    - usage guidelines.....549
  - no-logging statement
    - resource monitoring of memory blocks.....2034
  - no-more command.....732, 733
  - no-more filter.....595
  - nonpersistent statement.....1985
    - accounting
      - usage guidelines.....1682
  - Nontemporary Address
    - configuring.....1123
  - Nontemporary Addresses and Prefix
    - Delegation.....1124
  - nonvolatile statement.....2060
  - notify statement.....2085
    - usage guidelines.....1520
  - notify-filter statement
    - for applying to target.....2086
      - usage guidelines.....1527
    - for configuring.....2086
      - usage guidelines.....1522
  - notify-view statement.....2087
    - usage guidelines.....1515
  - NTP
    - listening
      - for broadcast messages.....1205
    - supported software standards.....2245
  - ntp statement.....1248
- O**
- object-names statement.....1985
  - objects-names statement
    - for Routing Engine profiles
      - usage guidelines.....1698
  - oid statement
    - SNMP.....2060
      - usage guidelines.....1496
    - SNMPv3.....2087
      - usage guidelines.....1522
  - Open Shortest Path First See OSPF

|                                                 |           |                                               |      |
|-------------------------------------------------|-----------|-----------------------------------------------|------|
| OpenFlow                                        |           | configuring on an interface.....              | 1933 |
| supported software standards.....               | 2265      | device interfaces supported.....              | 1928 |
| OpenFlow Switch Specification v1.0.0.....       | 2265      | disabling.....                                | 1940 |
| OpenFlow Switch Specification v1.3.1.....       | 2266      | disabling before changing encapsulation on    |      |
| openssl command.....                            | 771, 1028 | interfaces.....                               | 1941 |
| operating system See Junos OS                   |           | displaying configurations.....                | 1932 |
| operation statement.....                        | 1986      | displaying firewall filter for.....           | 1937 |
| for MIB profiles                                |           | enabling.....                                 | 1930 |
| usage guidelines.....                           | 1698      | encapsulation on interfaces, disabling before |      |
| operational mode, CLI                           |           | modifying.....                                | 1941 |
| command history.....                            | 454       | files See packet capture files                |      |
| switching to configuration mode.....            | 431       | firewall filters, configuring.....            | 1935 |
| users, monitoring.....                          | 571       | firewall filters, overview.....               | 1929 |
| word history.....                               | 454       | J-Web tool.....                               | 1947 |
| operational mode, filtering command output..... | 1397      | overview.....                                 | 1928 |
| operator login class permissions.....           | 795       | overview (J-Web).....                         | 1947 |
| operators                                       |           | preparation.....                              | 1930 |
| arithmetic, binary, and relational              |           | verifying captured packets.....               | 1932 |
| operators.....                                  | 1946      | verifying configuration.....                  | 1932 |
| logical.....                                    | 1946      | verifying firewall filter for.....            | 1937 |
| Optical Transport Network (OTN) Interface       |           | packet capture configuration                  |      |
| Management MIB. ....                            | 1434      | datapath debugging.....                       | 1937 |
| OSPF                                            |           | packet capture files                          |      |
| supported software standards.....               | 2284      | analyzing.....                                | 1929 |
| OSPF (Open Shortest Path First)                 |           | libpcap format.....                           | 1932 |
| monitoring.....                                 | 1823      | overview.....                                 | 1929 |
| statistics.....                                 | 1824      | renaming before modifying encapsulation on    |      |
| OSPF interfaces                                 |           | interfaces.....                               | 1941 |
| displaying.....                                 | 1824      | Packet Capture page                           |      |
| status.....                                     | 1824      | field summary.....                            | 1948 |
| OSPF MIB.....                                   | 1413      | results.....                                  | 1950 |
| OSPF neighbors                                  |           | packet encapsulation                          |      |
| displaying.....                                 | 1824      | troubleshooting on the link services          |      |
| status.....                                     | 1824      | interface.....                                | 1957 |
| OSPF routing information.....                   | 1823      | verifying on the link services interface..... | 1960 |
| OSPFv3                                          |           | packet filtering                              |      |
| supported software standards.....               | 2284      | supported software standards.....             | 2270 |
| outbound SSH service                            |           | Packet Forwarding Engine.....                 | 17   |
| configuring.....                                | 1064      | Packet Forwarding Engine MIB.....             | 1434 |
| outbound time See RPM probes                    |           | packet fragmentation                          |      |
| outbound-ssh statement                          |           | troubleshooting on the link services          |      |
| usage guidelines.....                           | 1064      | interface.....                                | 1957 |
| overrides statement                             |           | verifying on the link services interface..... | 1959 |
| DHCP local server.....                          | 1251      | Packet Mirror MIB.....                        | 1434 |
|                                                 |           | packet-capture statement.....                 | 1987 |
|                                                 |           | packet-filter statement                       |      |
|                                                 |           | security.....                                 | 1988 |
| <b>P</b>                                        |           |                                               |      |
| packet capture                                  |           |                                               |      |
| configuring.....                                | 1933      |                                               |      |
| configuring (J-Web).....                        | 1947      |                                               |      |

- packets
  - capturing.....1928
  - capturing with J-Web packet capture.....1947
  - monitoring jitter.....1736
  - monitoring packet loss.....1736
  - monitoring round-trip times.....1736
  - multicast, tracking .....1759
  - packet capture.....1928
  - packet capture (J-Web).....1947
  - tracking MPLS.....1920
  - tracking with J-Web traceroute.....1902
- PAE Extension MIB.....1434
- parameters statement.....2088
  - usage guidelines.....1526
- parentheses, in syntax descriptions.....lxiv
- partial command entry, completing.....710
- partitions, backing up.....322
- Passive Monitoring MIB.....1434
- password
  - root.....200, 204
  - root, setting .....200, 204
  - ssh public string.....201, 205
- password retry limits, setting.....1052
- passwords
  - for downloading software upgrades.....51, 150
  - local password method for user
    - authentication.....1022
    - See also local password
  - RADIUS.....1011
  - retry limits.....1052
  - setting login retry limits.....1052
  - srx root password, recovering.....1953
- paste command
  - usage guidelines.....458
- PC See management device
- PCAP See packet capture
- peer entities.....630
- peer statement.....1252
- peers, BGP See BGP neighbors; BGP RPM probes
- performance indicators.....1644
- performance, monitoring.....1656, 1715 See RPM
- permission bits, for login classes.....796
- permission flags
  - login class.....799
  - user.....799
- permissions
  - denying and allowing commands.....798
  - predefined.....795
- permissions statement
  - usage guidelines.....799
- permissions, CLI, displaying.....723, 1345
- PGM
  - supported software standards.....2276
- physical interfaces, summary information.....195
- PIC combinations
  - verifying during Junos OS installation.....269
- PIM
  - supported software standards.....2276
- PIM protocol, logging information.....195
- PIMs (Physical Interface Modules)
  - checking power and heat status.....1850
- ping
  - host reachability (CLI).....1912
  - host reachability (J-Web).....1914
  - ICMP probes.....1721
  - RPM probes See RPM probes
  - TCP and UDP probes.....1725
- ping command.....1912
  - network
    - connectivity, checking.....202, 206
  - options.....1912
- Ping end point of LSP
  - description.....1910
  - using.....1917
- Ping Host page
  - field summary.....1914
- Ping LDP-signaled LSP
  - description.....1910
  - using.....1917
- Ping LSP to Layer 3 VPN prefix
  - description.....1910
  - using.....1917
- Ping MIB.....1435
  - use in ping test.....1562
  - view configuration example
    - SNMP.....1497
- ping MPLS
  - options.....779
- ping MPLS (J-Web)
  - indications.....1920
  - Layer 2 circuits.....1909
  - Layer 2 VPNs.....1909
  - Layer 3 VPNs.....1909
  - LSP state.....1909
  - options.....1909, 1910
  - requirements.....1911
  - results.....1920

|                                                 |          |                                               |            |
|-------------------------------------------------|----------|-----------------------------------------------|------------|
| ping mpls l2circuit command.....                | 1921     | Power Supply Unit MIB.....                    | 1435       |
| results.....                                    | 1920     | PPP (Point-to-Point Protocol)                 |            |
| ping mpls l2vpn command.....                    | 1922     | monitoring (CLI).....                         | 1800       |
| results.....                                    | 1920     | PPP encapsulation                             |            |
| ping mpls l3vpn command.....                    | 1923     | on the link services interface.....           | 1960       |
| results.....                                    | 1920     | PPP interfaces                                |            |
| ping mpls ldp command.....                      | 1924     | supported software standards.....             | 2250       |
| results.....                                    | 1920     | PPP MIB.....                                  | 1413, 1435 |
| ping mpls lsp-end-point command.....            | 1924     | PPPoE (Point-to-Point Protocol over Ethernet) |            |
| results.....                                    | 1920     | interfaces.....                               | 1801       |
| Ping MPLS page                                  |          | monitoring.....                               | 1801       |
| field summary.....                              | 1917     | session status.....                           | 1801       |
| results.....                                    | 1920     | statistics.....                               | 1801       |
| ping mpls rsdp command.....                     | 1924     | version information.....                      | 1801       |
| results.....                                    | 1920     | PPPoE MIB.....                                | 1435       |
| Ping RSVP-signaled LSP                          |          | prefix list                                   |            |
| description.....                                | 1910     | adding to SNMP community.....                 | 1482       |
| using.....                                      | 1917     | prefix statement.....                         | 1253       |
| pingCtlTable.....                               | 1648     | Primary-level entry                           |            |
| pingProbeHistoryTable.....                      | 1567     | secondary-level entry.....                    | 1895       |
| pipe (   )                                      |          | Primary-level entry only.....                 | 1895       |
| command output, filtering.....                  | 590, 732 | privacy-3des statement.....                   | 2089       |
| pipe (l) command, to filter output.....         | 1397     | usage guidelines.....                         | 1511       |
| plain-text passwords                            |          | privacy-aes128 statement.....                 | 2090       |
| root password.....                              | 200, 204 | usage guidelines.....                         | 1510       |
| plain-text-password option.....                 | 200, 204 | privacy-des statement.....                    | 2091       |
| Point-to-Point Protocol See PPP                 |          | usage guidelines.....                         | 1511       |
| Point-to-Point Protocol over Ethernet See PPPoE |          | privacy-none statement.....                   | 2091       |
| Policy Objects MIB.....                         | 1435     | usage guidelines.....                         | 1511       |
| Port Activation License Support                 |          | privacy-password statement.....               | 2092       |
| MX104.....                                      | 228      | usage guidelines                              |            |
| port statement                                  |          | for 3DES algorithm.....                       | 1511       |
| SNMPv3.....                                     | 2088     | for AES algorithm.....                        | 1510       |
| usage guidelines.....                           | 1524     | for DES algorithm.....                        | 1511       |
| TACACS+                                         |          | probe loss                                    |            |
| usage guidelines.....                           | 1017     | monitoring.....                               | 1736       |
| usage guidelines.....                           | 1011     | threshold, setting.....                       | 1733       |
| ports                                           |          | probes, monitoring.....                       | 1736, 1801 |
| alarm conditions and configuration              |          | See also RPM probes                           |            |
| options.....                                    | 1705     | processes                                     |            |
| configuring alarms on.....                      | 1709     | managing.....                                 | 579        |
| console port, securing.....                     | 1051     | restarting.....                               | 740, 1338  |
| DHCP interface restrictions.....                | 1090     | processes, software                           |            |
| individual port types.....                      | 1705     | chassis process.....                          | 17         |
| monitoring.....                                 | 1794     | forwarding process.....                       | 17         |
| RADIUS servers.....                             | 1011     | interface process.....                        | 17         |
| power management, chassis.....                  | 1850     | management process.....                       | 17         |
| power supplies                                  |          | routing protocol process.....                 | 17         |
| environmental information.....                  | 192      |                                               |            |

- profiles, accounting
    - filter.....1687
    - interface.....1685
    - MIB.....1697
    - Routing Engine.....1699
  - programs
    - managing.....579
  - prompt
    - setting to display in CLI.....713
  - prompt strings
    - CLI.....646
  - protect command.....681
    - usage guidelines.....551
  - Protocol Independent Multicast *See* PIM
  - protocols
    - DHCP *See* DHCP
    - originating, displaying.....1821
    - OSPF, monitoring.....1823
    - PPP, monitoring.....1800
    - RIP, monitoring.....1822
    - routing protocols, monitoring.....1820, 1825
  - proxy ping
    - measurement tests.....1647
  - Pseudowire ATM MIB.....1435
  - Pseudowire TDM MIB.....1435
  - PSU MIB.....1435
  - PTP MIB.....1436
  - PVCs (permanent virtual circuits)
    - preventing dropped packets on.....1964
- Q**
- Quick Configuration
    - RPM pages.....1721
  - quit command.....564, 682
    - usage guidelines.....458
- R**
- RADIUS
    - authentication (configuration editor).....1014
    - order of user authentication (configuration editor).....1022
    - secret (configuration editor).....1014
    - specifying for authentication .....1022
    - supported software standards.....2244
  - RADIUS accounting.....1138
  - RADIUS authentication.....1011
    - security configuration example.....1011
  - RADIUS authorization *See* RADIUS authentication
  - radius-server statement
    - usage guidelines.....1011
  - rapid commit.....1125
  - rapid-commit statement.....1257
  - RARP, for autoinstallation.....84
  - re0 configuration group.....615
  - re1 configuration group.....615
  - read-only login class permissions.....795
  - read-view statement.....2093
    - usage guidelines.....1515
  - real-time performance monitoring *See* RPM
    - in service provider networks.....1647
  - Real-Time Performance Monitoring MIB.....1436
  - reboot immediately
    - with J-Web.....219
  - rebooting
    - with J-Web .....219
  - rebooting router software
    - requesting a system reboot.....309
    - requesting a system reboot with FreeBSD
      - upgrade.....316
  - reconfigure statement
    - DHCP local server.....1258
  - reconfiguring Junos OS .....198
  - recovery software installation.....42
    - procedures.....172
  - red asterisk (\*).....764
  - redrawing screen.....600
  - redundancy-group statement.....1989
  - redundant Ethernet interface LAG.....1745
  - regional configurations.....631
  - registration form, for software upgrades.....147
  - regular expressions
    - first match, displaying from.....594
    - matching output, displaying.....595
    - nonmatching output, ignoring.....593
  - reinstall Junos OS
    - checklist.....187
    - comparing configurations.....206, 207
    - steps .....197
  - reinstalling Junos OS.....172
  - relational operators, for multicast traffic.....1946
  - relative option.....546
  - release names.....11
  - remote accounts
    - accessing with SSH (CLI).....1063
    - accessing with Telnet (CLI).....1062
    - remote template accounts.....810

|                                                  |                            |  |
|--------------------------------------------------|----------------------------|--|
| remote connection to router                      |                            |  |
| connecting USB modem to router.....              | 1038                       |  |
| Remote Monitoring.....                           | 2203                       |  |
| remote operations MIBs.....                      | 1561                       |  |
| remote server, upgrading from.....               | 65, 152                    |  |
| remote template accounts.....                    | 810                        |  |
| remote-engine statement.....                     | 2094                       |  |
| removable media                                  |                            |  |
| booting from.....                                | 36                         |  |
| reinstalling Junos OS, using.....                | 172                        |  |
| removing                                         |                            |  |
| files.....                                       | 1312                       |  |
| software packages.....                           | 347                        |  |
| rename command.....                              | 683                        |  |
| example configuration.....                       | 476                        |  |
| usage guidelines.....                            | 476                        |  |
| renaming files.....                              | 1314                       |  |
| renaming identifiers.....                        | 476                        |  |
| replace command.....                             | 684                        |  |
| example configuration.....                       | 476                        |  |
| global.....                                      | 606                        |  |
| usage guidelines.....                            | 603                        |  |
| replace option.....                              | 545                        |  |
| req-option statement.....                        | 1259                       |  |
| request command.....                             | 735                        |  |
| usage guidelines.....                            | 564                        |  |
| request interface modem reset umd0               |                            |  |
| command.....                                     | 1050                       |  |
| request message filter.....                      | 595                        |  |
| request pppoe connect command.....               | 2123                       |  |
| request pppoe disconnect command.....            | 2124                       |  |
| request security idp security-package download   |                            |  |
| command.....                                     | 307                        |  |
| request snmp spoof-trap command.....             | 2126                       |  |
| request system autorecovery state                |                            |  |
| command.....                                     | 292, 1318                  |  |
| request system configuration rescue delete       |                            |  |
| command.....                                     | 538, 549                   |  |
| request system configuration rescue save         |                            |  |
| command.....                                     | 538, 549                   |  |
| request system decrypt password.....             | 1320                       |  |
| request system download abort                    |                            |  |
| command.....                                     | 294, 1321                  |  |
| request system download clear                    |                            |  |
| command.....                                     | 295, 1322                  |  |
| request system download pause                    |                            |  |
| command.....                                     | 296, 1323                  |  |
| request system download resume                   |                            |  |
| command.....                                     | 297, 1324                  |  |
| request system download start                    |                            |  |
| command.....                                     | 298, 1325                  |  |
| request system firmware upgrade                  |                            |  |
| command.....                                     | 299, 1326                  |  |
| request system halt.....                         | 300                        |  |
| request system halt command.....                 | 583                        |  |
| request system license add                       |                            |  |
| command.....                                     | 257, 302, 1154             |  |
| request system license add terminal              |                            |  |
| command.....                                     | 257, 1154                  |  |
| request system license delete                    |                            |  |
| command.....                                     | 258, 303, 1157             |  |
| request system license save                      |                            |  |
| command.....                                     | 259, 304, 1153             |  |
| request system license update                    |                            |  |
| command.....                                     | 305, 1154, 1327            |  |
| request system logout pid pid_number             |                            |  |
| command.....                                     | 467                        |  |
| request system partition compact-flash           |                            |  |
| command.....                                     | 306                        |  |
| request system power-off fpc command.....        | 1328                       |  |
| request system reboot.....                       | 1334                       |  |
| request system reboot (FreeBSD upgrade)          |                            |  |
| command.....                                     | 316                        |  |
| request system reboot command.....               | 309, 583                   |  |
| request system services dhcp command.....        | 1329                       |  |
| request system set-encryption-key algorithm des  |                            |  |
| command.....                                     | 1132                       |  |
| request system set-encryption-key                |                            |  |
| command.....                                     | 1132                       |  |
| request system set-encryption-key des            |                            |  |
| unique.....                                      | 1132                       |  |
| request system set-encryption-key unique.....    | 1132                       |  |
| request system snapshot.....                     | 42, 331, 1330              |  |
| request system snapshot                          |                            |  |
| command.....                                     | 55, 56, 197, 207, 208, 322 |  |
| request system snapshot command (upgraded        |                            |  |
| FreeBSD).....                                    | 329                        |  |
| request system snapshot media command.....       | 55                         |  |
| request system snapshot slice alternate          |                            |  |
| command.....                                     | 55                         |  |
| request system software abort in-service-upgrade |                            |  |
| command.....                                     | 333, 1332                  |  |
| request system software add .....                | 344, 1333                  |  |
| request system software add command.....         | 334                        |  |
| request system software delete command.....      | 347                        |  |
| request system software rollback.....            | 42, 356, 1335              |  |
| request system software rollback command.....    | 351                        |  |
| request system software validate command.....    | 357                        |  |

- 
- request system software validate command
    - (upgraded FreeBSD).....361
  - request system storage cleanup
    - command.....364, 374, 1135
  - request system storage cleanup dry-run
    - command.....1135
  - request system zeroize command.....377
  - request-type statement.....2025
    - RMON
      - usage guidelines.....1629
  - required entry .....764
  - rescue configuration file
    - saving.....183
  - rescue configuration, alarm about.....1708
  - resolve command.....732
  - resource monitoring
    - configuration.....2031
  - Resource Reservation Protocol *See* RSVP *See* RSVP
  - resource-monitor statement
    - resource monitoring of memory blocks.....2035
  - resource-type contiguous-pages statement
    - resource monitoring of memory blocks.....2036
  - resource-type free-dwords statement
    - resource monitoring of memory blocks.....2037
  - resource-type free-pages statement
    - resource monitoring of memory blocks.....2038
  - restart command.....740, 1338
    - usage guidelines.....564
  - restart routing command.....582
  - restarting
    - after software upgrade.....646
    - software processes.....740, 1338
  - restoring a saved router configuration.....184
  - reth
    - link aggregation group.....1745
  - retransmission-attempt statement.....1260
  - retransmission-interval (dhcp-client)
    - statement.....1261
  - retry limits for passwords.....1052
  - retry statement
    - usage guidelines.....1011
  - retry-count statement.....2081
    - usage guidelines.....1534
  - retry-interval statement.....1990
  - Reverse Address Resolution Protocol (RARP), for
    - autoinstallation.....84
  - Reverse-Path-Forwarding MIB.....1436
  - reverting to a previous configuration file
    - (J-Web).....156
  - reverting to earlier software.....352
  - RFC 1542, Clarifications and Extensions for the
    - Bootstrap Protocol.....2232
  - RFC 3719, Recommendations for Interoperable
    - Networks using Intermediate System to
      - Intermediate System (IS-IS).....2283
  - RFC 4087, IP Tunnel MIB.....2241
  - RFC 4133, Entity MIB.....2241
  - RFC 4364, BGP/MPLS IP Virtual Private Networks
    - (VPNs).....2259, 2274, 2278, 2293, 2294, 2295
  - RFC 4382, MPLS/BGP Layer 3 Virtual Private
    - Network (VPN) MIB .....2241
  - RFC 4444, Management Information Base for
    - Intermediate System to Intermediate System
      - (IS-IS).....2242
  - RFC 4717, Encapsulation Methods for Transport of
    - Asynchronous Transfer Mode (ATM) over MPLS
      - Networks.....2247
  - RFC 4761, Virtual Private LAN Service (VPLS) Using
    - BGP for Auto-Discovery and
      - Signaling.....2294, 2296
  - RFC 5187, OSPFv3 Graceful Restart.....2285
  - RFC 5317, Joint Working Team (JWT) Report on
    - MPLS Architectural Considerations for a
      - Transport Profile .....2260
  - RFC 5340, OSPF for IPv6.....2280, 2284
  - RFC 5586, MPLS Generic Associated
    - Channel.....2260
  - RFC 5654, Requirements of an MPLS Transport
    - Profile.....2260
  - RFC 5712, MPLS Traffic Engineering Soft
    - Preemption.....2260
  - RFC 5718, An In-Band Data Communication
    - Network For the MPLS Transport Profile.....2260
  - RFC 5860, Requirements for Operations,
    - Administration, and Maintenance (OAM) in MPLS
      - Transport Networks.....2260
  - RFC 5921, A Framework for MPLS in Transport
    - Networks.....2260
  - RFC 5950, Network Management Framework for
    - MPLS-based Transport Networks.....2260
  - RFC 5951, Network Management Requirements for
    - MPLS-based Transport Networks.....2260
  - RFC 5960, MPLS Transport Profile Data Plane
    - Architecture.....2260
  - RFC 6215, MPLS Transport Profile User-to-Network
    - and Network-to-Network Interfaces.....2260
  - RFC 6291, Guidelines for the Use of the "OAM"
    - Acronym in the IETF.....2260



|                                                                                                                                  |            |
|----------------------------------------------------------------------------------------------------------------------------------|------------|
| RFC 6370, MPLS Transport Profile (MPLS-TP)                                                                                       |            |
| Identifiers .....                                                                                                                | 2260       |
| RFC 6371, Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks.....                           | 2260       |
| RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths ..... | 2260       |
| RFC 6424, Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels.....                                    | 2260       |
| RFC 6425, Detecting Data-Plane Failures in Point-to-Multipoint MPLS - Extensions to LSP Ping .....                               | 2261       |
| RFC 6426, MPLS On-demand Connectivity Verification and Route Tracing.....                                                        | 2261       |
| RFC 6428, Proactive Connectivity Verification, Continuity Check and Remote Defect Indication for MPLS Transport Profile .....    | 2261       |
| RFC 7432, BGP MPLS-Based Ethernet VPN.....                                                                                       | 2294       |
| RFCs supported See Index of Supported Software Standards                                                                         |            |
| RIP                                                                                                                              |            |
| supported software standards.....                                                                                                | 2286       |
| RIP (Routing Information Protocol)                                                                                               |            |
| monitoring.....                                                                                                                  | 1822       |
| statistics.....                                                                                                                  | 1822       |
| RIP neighbors                                                                                                                    |            |
| displaying.....                                                                                                                  | 1822       |
| status.....                                                                                                                      | 1822       |
| RIP routing information.....                                                                                                     | 1822       |
| RIPng                                                                                                                            |            |
| supported software standards.....                                                                                                | 2286       |
| rising-event-index statement.....                                                                                                | 2026       |
| usage guidelines.....                                                                                                            | 1627       |
| rising-threshold statement                                                                                                       |            |
| health monitor.....                                                                                                              | 2017       |
| RMON.....                                                                                                                        | 2026       |
| RMON alarm entries.....                                                                                                          | 1626       |
| RMON alarms.....                                                                                                                 | 1621, 1641 |
| RMON alarms and events, displaying.....                                                                                          | 2203       |
| RMON event entries.....                                                                                                          | 1630       |
| RMON events.....                                                                                                                 | 1623, 1640 |
| RMON Events and Alarms MIB.....                                                                                                  | 1436       |
| rmon statement.....                                                                                                              | 2027       |
| usage guidelines.....                                                                                                            | 1640       |
| roles                                                                                                                            |            |
| example.....                                                                                                                     | 815        |
| rollback                                                                                                                         |            |
| requesting.....                                                                                                                  | 351        |
| rollback command.....                                                                                                            | 444, 685   |
| usage guidelines.....                                                                                                            | 458        |
| rolling back a configuration file, to downgrade software (CLI).....                                                              | 156        |
| root                                                                                                                             |            |
| file system, backing up.....                                                                                                     | 197        |
| root login to the console, disabling.....                                                                                        | 1051       |
| root password.....                                                                                                               | 200, 204   |
| root password recovery.....                                                                                                      | 1953       |
| root-authentication statement                                                                                                    |            |
| usage guidelines.....                                                                                                            | 200, 204   |
| rotating files.....                                                                                                              | 1134       |
| round-trip time                                                                                                                  |            |
| description.....                                                                                                                 | 1717       |
| See also RPM probes                                                                                                              |            |
| threshold, setting.....                                                                                                          | 1733       |
| router.conf file, for autoinstallation.....                                                                                      | 83         |
| routers                                                                                                                          |            |
| active configuration, logging .....                                                                                              | 194        |
| boot sequence.....                                                                                                               | 15         |
| M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, ACX Series, and PTX Series routing engines.....                        | 34         |
| chassis                                                                                                                          |            |
| hardware version, logging .....                                                                                                  | 190        |
| check network connectivity.....                                                                                                  | 201, 206   |
| configuring name and address.....                                                                                                | 198, 202   |
| copying backup configuration .....                                                                                               | 202, 206   |
| environment, logging.....                                                                                                        | 191        |
| interfaces, logging.....                                                                                                         | 194        |
| model, logging .....                                                                                                             | 190        |
| ports                                                                                                                            |            |
| RADIUS servers.....                                                                                                              | 1011       |
| storage media.....                                                                                                               | 30         |
| routing                                                                                                                          |            |
| monitoring.....                                                                                                                  | 1820       |
| traceroute (J-Web).....                                                                                                          | 1902       |
| Routing Engine                                                                                                                   |            |
| environment information.....                                                                                                     | 192        |
| software component.....                                                                                                          | 17         |
| Upgrade to 64-bit Junos OS.....                                                                                                  | 119        |
| Routing Engine profile.....                                                                                                      | 1699       |
| Routing Engine traffic from trusted sources                                                                                      |            |
| stateless firewall filters                                                                                                       |            |
| blocking Telnet and SSH access.....                                                                                              | 1057       |



- 
- Routing Engines
    - available disk space, managing.....269
    - backup
      - installing software.....59
    - illustrations.....29
    - master
      - installing software.....61
    - storage media
      - ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS routers.....32
    - synchronizing configuration.....558
  - routing instances
    - access lists
      - configuring.....1557
    - SNMP
      - enabling access.....1555
      - identifying.....1554
      - specifying.....1555
  - routing protocol software process.....17
  - routing solutions
    - applying CoS components on link services
      - interface.....1955
    - load balancing on link services
      - interfaces.....1957
    - preventing dropped packets on PVCs.....1964
    - reducing jitter and latency on multilink bundles.....1957
  - routing table
    - monitoring.....1820
  - routing-engine-profile statement.....1991
    - usage guidelines.....1699
  - routing-instance statement
    - SNMP.....2062
    - SNMPv3.....2095
      - usage guidelines.....1524
    - usage guidelines.....1011
  - routing-instance-access.....2063
  - RPC
    - displaying command output in.....593
  - rpd process.....17
  - RPM
    - supported software standards.....2291
  - RPM (real-time performance monitoring)
    - basic probes (configuration editor).....1721
    - BGP monitoring *See* BGP RPM probes
    - inbound and outbound times.....1717
    - IPv6 probes (configuration editor).....1731
    - jitter, viewing.....1736
    - monitoring probes.....1736
    - overview.....1715
      - See also* RPM probes
    - preparation.....1721
    - probe and test intervals.....1716
    - probe counts.....1717
    - Quick Configuration.....1721
    - round-trip times, description.....1717
    - round-trip times, viewing.....1736
    - sample configuration.....1724
    - sample graphs.....1736
    - statistics.....1717
    - statistics, verifying.....1724
    - TCP probes (configuration editor).....1725
      - See also* TCP RPM probes
    - tests.....1716
    - tests, viewing.....1736
    - threshold values.....1718
    - tuning probes.....1732
    - UDP probes (configuration editor).....1725
      - See also* UDP RPM probes
    - verifying probe servers.....1727
  - RPM MIB.....1436
  - RPM pages.....1721
    - field summary.....1733
  - RPM probe timestamps
    - overview.....1716
    - setting (configuration editor).....1721
  - RPM probes
    - basic (configuration editor).....1721
    - BGP neighbors *See* BGP RPM probes
    - cumulative jitter.....1736
    - current tests.....1736
    - DSCP bits (Quick Configuration).....1733
    - graph results.....1736
    - ICMP (configuration editor).....1721
    - ICMPv6 (configuration editor).....1731
    - inbound times.....1717
    - IPv6 (configuration editor).....1731
    - jitter threshold.....1733
    - monitoring.....1736
    - outbound times.....1717
    - probe count, setting (Quick Configuration).....1733
    - probe count, tuning.....1732
    - probe counts.....1717
    - probe intervals.....1716
    - probe intervals, setting (Quick Configuration).....1733

|                                                         |      |                                                            |               |
|---------------------------------------------------------|------|------------------------------------------------------------|---------------|
| probe intervals, tuning.....                            | 1732 | local template account.....                                | 810           |
| probe loss count.....                                   | 1733 | RPM probes.....                                            | 1724          |
| probe owner.....                                        | 1733 | RPM test graphs.....                                       | 1736          |
| probe type, setting (Quick<br>Configuration).....       | 1733 | TCP and UDP probes.....                                    | 1725          |
| probe types.....                                        | 1716 | user account.....                                          | 807           |
| round-trip time threshold.....                          | 1733 | SAP                                                        |               |
| round-trip times, description.....                      | 1717 | supported software standards.....                          | 2276          |
| round-trip times, viewing.....                          | 1736 | save command.....                                          | 687, 732      |
| SNMP traps (Quick Configuration).....                   | 1733 | usage guidelines.....                                      | 458, 539, 540 |
| source address, setting.....                            | 1732 | saving licenses (CLI).....                                 | 259, 1153     |
| TCP (configuration editor).....                         | 1725 | saving rescue configuration file.....                      | 183           |
| See also TCP RPM probes                                 |      | scheduling a reboot<br>with J-Web.....                     | 219           |
| TCP server port.....                                    | 1733 | screen                                                     |               |
| test intervals.....                                     | 1716 | dimensions.....                                            | 645, 647      |
| test intervals, setting (Quick<br>Configuration).....   | 1733 | redrawing.....                                             | 600           |
| test target.....                                        | 1733 | screen length, setting.....                                | 715           |
| threshold values, description.....                      | 1718 | screen width, setting.....                                 | 716           |
| threshold values, setting (Quick<br>Configuration)..... | 1733 | SDH                                                        |               |
| timestamps See RPM probe timestamps                     |      | supported software standards.....                          | 2251          |
| tuning.....                                             | 1732 | SDP                                                        |               |
| UDP (configuration editor).....                         | 1725 | supported software standards.....                          | 2276          |
| See also UDP RPM probes                                 |      | secret                                                     |               |
| UDP server port.....                                    | 1733 | RADIUS (configuration editor).....                         | 1014          |
| verifying TCP and UDP probe servers.....                | 1727 | TACACS+ (configuration editor).....                        | 1019          |
| RSVP                                                    |      | secret statement                                           |               |
| supported software standards.....                       | 2262 | authentication                                             |               |
| RSVP (Resource Reservation Protocol)                    |      | usage guidelines, RADIUS.....                              | 1011          |
| interfaces, monitoring.....                             | 1799 | usage guidelines, TACACS+.....                             | 1017          |
| sessions, monitoring.....                               | 1798 | secure access                                              |               |
| RSVP MIB.....                                           | 1436 | establishing.....                                          | 1027          |
| RSVP protocol, logging information.....                 | 195  | generating SSL certificates.....                           | 1028          |
| RTT See RPM probes, round-trip times                    |      | HTTPS access .....                                         | 1029          |
| run command.....                                        | 686  | HTTPS access (configuration editor).....                   | 1031          |
| usage guidelines.....                                   | 458  | HTTPS recommended.....                                     | 771, 1027     |
|                                                         |      | installing SSL certificates.....                           | 1029          |
|                                                         |      | installing SSL certificates (configuration<br>editor)..... | 1031          |
|                                                         |      | Junos XML protocol SSL access.....                         | 1029          |
|                                                         |      | overview.....                                              | 1027          |
|                                                         |      | requirements.....                                          | 1028          |
|                                                         |      | sample configuration.....                                  | 1032          |
|                                                         |      | verifying secure access configuration.....                 | 1032          |
|                                                         |      | Secure Sockets Layer See SSL                               |               |
|                                                         |      | security                                                   |               |
|                                                         |      | access privileges.....                                     | 795, 807      |
|                                                         |      | alarms.....                                                | 2174          |
|                                                         |      | console port security.....                                 | 1051          |
|                                                         |      | packet capture for intrusion detection.....                | 1928          |

## S

|                            |      |
|----------------------------|------|
| sample configuration       |      |
| for secure access.....     | 1032 |
| for SSL certificates.....  | 1032 |
| sample-type statement..... | 2027 |
| usage guidelines           |      |
| for alarms.....            | 1629 |
| for events.....            | 1630 |
| samples                    |      |
| alarm configuration.....   | 1711 |
| basic RPM probes.....      | 1721 |

- password retry limits.....1052
- user accounts.....798, 807
- user authentication.....804
- Security Interface Extension Objects MIB.....1436
- security policy
  - DNS name resolution.....1954
- Security Screening Objects MIB.....1437
- security-level statement
  - for access privileges.....2096
  - usage guidelines.....1514
  - for SNMP notifications.....2097
  - usage guidelines.....1528
- security-model statement
  - for access privileges.....2098
  - usage guidelines.....1514
  - for groups.....2099
  - usage guidelines.....1517
  - for SNMP notifications.....2099
  - usage guidelines.....1528
- security-name statement
  - for community string.....2100
  - for security group.....2101
  - usage guidelines.....1518
  - for SNMP notifications.....2102
  - usage guidelines.....1528
- security-to-group statement.....2103
- usage guidelines.....1512
- serial cable, disconnection for console logout.....1051
- serial interfaces
  - supported software standards.....2252
- Serial Line Address Resolution Protocol (SLARP),
  - for autoinstallation.....84
- serial ports
  - alarm conditions and configuration
    - options.....1705
  - autoinstallation on.....82
  - configuring alarms on.....1709
- server address statement.....1265
- server statement
  - NTP.....1264
- service quality
  - monitoring.....1643
- service-name statement.....1271
- Services Gateway
  - licenses.....1145
- services module
  - alarm conditions and configuration
    - options.....1705
- Services PIC MIB.....1437
- Services Router
  - as a DHCP server.....1088
  - licenses.....1145
  - monitoring .....1397
  - performance monitoring.....1715
- services statement
  - resource monitoring of memory blocks.....2039
- sessions
  - BGP peer, status details.....1825
  - limits.....785
  - RSVP, monitoring.....1798
  - Telnet.....1062
  - terminating.....785
- sessions, J-Web.....772
- set cli complete-on-space command.....710
- usage guidelines.....647
- set cli directory command.....711
- usage guidelines.....646
- set cli idle-timeout command.....712
- usage guidelines.....646
- set cli prompt command.....713
- usage guidelines.....646
- set cli restart-on-upgrade command.....714
- usage guidelines.....646
- set cli screen-length command.....715
- usage guidelines.....645, 647
- set cli screen-width command.....716
- set cli terminal command.....717
- usage guidelines.....646
- set cli timestamp command.....718
- usage guidelines.....646
- set command.....469
- configuration mode.....689, 751
- usage guidelines.....458
- set date command.....719
- set interfaces address command .....199, 202
- set no-encrypt-configuration-files command.....1132
- set option.....546
- set system backup-router command.....199, 203
- set system domain-name command.....199, 202
- set system host-name command.....198, 202
- set system name-server command.....199, 203
- set system root-authentication
  - command.....201, 205
- set system root-authentication
  - encrypted-password command.....201, 205
- Set Up page
  - field summary.....777
- setting root password.....200, 204

|                                             |                           |
|---------------------------------------------|---------------------------|
| severity levels                             |                           |
| for alarms See alarm severity               |                           |
| SHA-1 (Secure Hash Algorithm) checksum..... | 11                        |
| sha-256 checksum, calculating.....          | 1306                      |
| SHA-1 checksum, calculating.....            | 1305                      |
| show bgp neighbor command.....              | 1825                      |
| show bgp summary command.....               | 195, 206, 207, 1825       |
| show chassis alarms command.....            | 1711, 2132                |
| show chassis cluster ip-monitoring status   |                           |
| redundancy-group command.....               | 2134                      |
| show chassis environment                    |                           |
| command.....                                | 191, 206, 207, 1850       |
| show chassis hardware command               |                           |
| .....                                       | 190, 206, 207, 1848, 1850 |
| show chassis power-ratings command.....     | 1850                      |
| show chassis redundant-power-supply         |                           |
| command.....                                | 1850                      |
| show chassis routing-engine.....            | 29                        |
| show chassis routing-engine bios.....       | 69                        |
| show chassis routing-engine                 |                           |
| command.....                                | 1343, 1850                |
| show chassis usb storage command.....       | 382                       |
| show cli authorization command.....         | 723, 1345                 |
| show cli command.....                       | 720, 722                  |
| usage guidelines.....                       | 647                       |
| show cli directory command.....             | 724                       |
| show cli history command.....               | 725                       |
| usage guidelines.....                       | 454                       |
| show command                                |                           |
| configuration mode.....                     | 690                       |
| usage guidelines.....                       | 458                       |
| show configuration command.....             | 691                       |
| log active.....                             | 194, 206, 207             |
| show dhcpv6 server binding.....             | 1363                      |
| show dhcpv6 server statistics command.....  | 1367                      |
| show firewall command.....                  | 1370                      |
| show firewall filter dest-all command.....  | 1937                      |
| show groups junos-defaults command.....     | 698                       |
| usage guidelines.....                       | 640                       |
| show ilmi statistics command.....           | 2171                      |
| show interface terse command.....           | 194, 206, 207             |
| show interfaces command.....                | 2137                      |
| show interfaces detail command.....         | 1794                      |
| show interfaces dlo extensive command.....  | 1045                      |
| show interfaces interface-name command..... | 1794                      |
| show interfaces pp0 command.....            | 1801                      |
| show interfaces snmp-index command.....     | 2168                      |
| show interfaces summary.....                | 2169                      |
| show interfaces terse command.....          | 1794                      |
| show isis adjacency brief command.....      | 195, 206, 207             |
| show mpls interface command.....            | 1796                      |
| show mpls lsp command.....                  | 1796                      |
| show mpls statistics command.....           | 1797                      |
| show ospf interfaces command.....           | 1823                      |
| show ospf neighbor brief command.....       | 195, 206, 207             |
| show ospf neighbors command.....            | 1823                      |
| show ospf statistics command.....           | 1823                      |
| show ppp address-pool command.....          | 1800                      |
| show ppp interface command.....             | 1800                      |
| show ppp statistics command.....            | 1800                      |
| show ppp summary command.....               | 1800                      |
| show pppoe interfaces command.....          | 1801                      |
| show pppoe statistics command.....          | 1801                      |
| show pppoe version command.....             | 1801                      |
| show redundant-power-supply command.....    | 1850                      |
| show rip neighbors command.....             | 1822                      |
| show rip statistics command.....            | 1822                      |
| show route command.....                     | 202, 206                  |
| show route detail command.....              | 1820                      |
| show route terse command.....               | 1820                      |
| show security alarms command.....           | 2174                      |
| show security datapath-debug capture.....   | 2178                      |
| show security datapath-debug counter.....   | 2179                      |
| show security monitoring fpc fpc-number     |                           |
| command.....                                | 2182                      |
| show services ip-monitoring status          |                           |
| command.....                                | 2187                      |
| show services rpm active-servers            |                           |
| command.....                                | 1727, 1730                |
| explanation.....                            | 1727, 1730                |
| show services rpm probe-results             |                           |
| command.....                                | 1724, 1736                |
| explanation.....                            | 1724                      |
| show snmp health-monitor command.....       | 2191                      |
| show snmp inform-statistics command.....    | 2198                      |
| show snmp mib command.....                  | 2200                      |
| show snmp rmon command.....                 | 2203                      |
| show snmp statistics command.....           | 2207                      |
| show snmp stats-response-statistics         |                           |
| command.....                                | 2215                      |
| show snmp v3 command.....                   | 2217                      |
| show system alarms command.....             | 2220                      |
| show system auto-snapshot status            |                           |
| command.....                                | 394                       |
| show system autoinstallation status         |                           |
| command.....                                | 86, 383                   |
| show system autorecovery state              |                           |
| command.....                                | 385, 1372                 |

- show system boot-messages
  - command.....192, 206, 207, 387
- show system download command.....396, 1374
- show system license
  - command.....260, 398, 406, 1156, 1158, 1376
  - explanation.....260, 1156, 1158
- show system license keys command.....1156
- show system license usage command.....261, 1156
  - explanation.....261, 1156
- show system login lockout command.....409, 1379
- show system processes extensive command.....580
  - output, table.....581
- show system resource-monitor command.....2221
- show system services dhcp client command.....1380
- show system services dhcp conflict
  - command.....1089
- show system services dhcp relay-statistics
  - command.....1383
- show system snapshot command.....410
- show system snapshot command (FreeBSD upgrade).....413
- show system snapshot media.....168, 414, 1385
- show system storage.....34
- show system storage
  - command.....196, 206, 207, 1848
- show system storage partitions.....417, 1386
- show system uptime command.....1848
- show system users command.....1848
- show version.....48
- show version command.....48, 189, 1848
  - compare information .....206, 207
  - Junos OS.....578
  - reinstalling software.....189
- show | display inheritance command.....694
- show | display omit command.....695
- show | display set command.....696
  - usage guidelines.....501
- show | display set relative command.....697
  - usage guidelines.....502
- show forwarding-options command.....1932
- single-connection statement
  - usage guidelines.....1017
- SIP
  - supported software standard.....2291
- size statement
  - accounting.....1992
  - usage guidelines.....1683
- SLARP, for autoinstallation.....84
- snapshots
  - FreeBSD upgrade.....23
- SNMP.....1485
  - adding client lists and prefix lists.....1482
  - commit delay timer.....1478
  - community string.....1479
  - configuration
    - version 3.....1500
  - FAQs
    - troubleshooting.....1591
  - filtering duplicate requests.....1478
  - health monitor alarms, displaying.....2191
  - inform statistics, displaying.....2198
  - limiting interface access.....1494
  - logging, enabling.....1562
  - MIB object values, displaying.....2200
  - MIB views.....1496
  - remote operations.....1559
  - RMON alarms and events, displaying.....2203
  - standards documents.....1409
  - statistics
    - clearing.....2121
    - displaying.....2207
  - system contact.....1474, 1476
  - system description.....1475, 1476
  - system location.....1475, 1476, 2057
  - system name.....1477
  - tracing operations.....1585
  - trap groups.....1491
  - trap notification for remote operations.....1561
  - trap options.....1487
  - version 3 configuration, displaying.....2217
  - views, setting.....1560
- SNMP FAQs
  - troubleshooting
    - best practices.....1592
- snmp history
  - clear.....2120
- SNMP index
  - interface information, displaying.....2168
- SNMP inform notifications
  - example configuration.....1531
- SNMP inform statistics, displaying.....2198
- SNMP informs.....1529
- snmp statement.....2063
  - usage guidelines
    - SNMPv3.....1500

|                                                                                 |      |
|---------------------------------------------------------------------------------|------|
| SNMP traps                                                                      |      |
| performance monitoring See RPM probes                                           |      |
| source address configuration.....                                               | 1488 |
| spoofing.....                                                                   | 2126 |
| snmp-community statement.....                                                   | 2103 |
| SNMPv2                                                                          |      |
| Passive Monitoring Traps MIB.....                                               | 1491 |
| SNMPv3                                                                          |      |
| authentication, configuring.....                                                | 1509 |
| informs, configuring.....                                                       | 1529 |
| local engine ID, configuring.....                                               | 1506 |
| minimum configuration.....                                                      | 1502 |
| SNMPv3 context                                                                  |      |
| usage guidelines.....                                                           | 1538 |
| software.....                                                                   | 17   |
| halting immediately (J-Web) .....                                               | 219  |
| <i>See also</i> Junos OS                                                        |      |
| software categories                                                             |      |
| on M Series, MX Series, T Series, TX Matrix, and<br>TX Matrix Plus routers..... | 42   |
| software installation                                                           |      |
| category change installation                                                    |      |
| description.....                                                                | 41   |
| recovery installation                                                           |      |
| description.....                                                                | 42   |
| standard installation                                                           |      |
| description.....                                                                | 41   |
| software installation packages                                                  |      |
| Junos OS for SRX devices, domestic                                              |      |
| description.....                                                                | 43   |
| Junos OS for SRX devices, export                                                |      |
| description.....                                                                | 43   |
| Junos-FIPS                                                                      |      |
| description.....                                                                | 42   |
| standard Junos OS, domestic                                                     |      |
| description.....                                                                | 42   |
| standard Junos OS, export                                                       |      |
| description.....                                                                | 42   |
| software package names                                                          |      |
| FreeBSD upgrade.....                                                            | 22   |
| software packages                                                               |      |
| upgrading individual.....                                                       | 116  |
| software, Junos                                                                 |      |
| backing up .....                                                                | 207  |
| checklist for reinstalling.....                                                 | 187  |
| logging hardware version.....                                                   | 190  |
| logging software version .....                                                  | 189  |
| packages                                                                        |      |
| logging .....                                                                   | 189  |
| reconfiguring.....                                                              | 198  |
| reinstalling.....                                                               | 197  |
| SONET                                                                           |      |
| supported software standards.....                                               | 2251 |
| SONET APS MIB.....                                                              | 1437 |
| SONET Automatic Protection Switching MIB.....                                   | 1437 |
| SONET/SDH Interface Management MIB.....                                         | 1437 |
| Source Class Usage MIB.....                                                     | 1437 |
| source-address statement.....                                                   | 2064 |
| NTP.....                                                                        | 1265 |
| RADIUS                                                                          |      |
| usage guidelines.....                                                           | 1011 |
| RADIUS and TACACS+.....                                                         | 1265 |
| system logging.....                                                             | 1265 |
| usage guidelines.....                                                           | 1488 |
| usage guidelines, RADIUS.....                                                   | 1011 |
| source-classes statement.....                                                   | 1992 |
| usage guidelines.....                                                           | 1695 |
| SPU Monitoring MIB.....                                                         | 1437 |
| SRX Series.....                                                                 | 1131 |
| alarms.....                                                                     | 1703 |
| licenses.....                                                                   | 1145 |
| managing user authentication.....                                               | 804  |
| monitoring .....                                                                | 1397 |
| packet capture.....                                                             | 1928 |
| performance monitoring.....                                                     | 1715 |
| SRX series device                                                               |      |
| bring components online/offline.....                                            | 213  |
| halting.....                                                                    | 213  |
| rebooting.....                                                                  | 213  |
| SRX series devices                                                              |      |
| software upgrades.....                                                          | 146  |
| SRX Series Services Gateway.....                                                | 166  |
| <i>See</i> storage                                                              |      |
| m e d i a                                                                       |      |
| auto bios upgrade methods.....                                                  | 155  |
| Chassis Components                                                              |      |
| Offline.....                                                                    | 218  |
| Online.....                                                                     | 218  |
| configuring boot devices.....                                                   | 166  |
| dual-root partitioning.....                                                     | 105  |
| Install Remote page                                                             |      |
| field summary.....                                                              | 166  |
| installing software                                                             |      |
| with CLI.....                                                                   | 110  |
| with J-Web.....                                                                 | 110  |
| Junos OS Release 10.0                                                           |      |
| upgrading without dual-root.....                                                | 146  |
| show system storage partitions.....                                             | 113  |

- snapshots.....166
- software upgrade methods.....146
- See also boot devices
- SSH
  - accessing remote accounts (CLI).....1063
  - setting login retry limits.....1052
- ssh command.....1063
  - options.....1063
  - usage guidelines.....564
- SSH key files.....200, 204
- ssh-known-hosts statement.....1266
- SSL (Secure Sockets Layer)
  - enabling secure access .....1029
  - management access.....1027
  - verifying SSL configuration.....1032
- SSL access, establishing.....1027
- SSL certificates
  - adding.....1033
  - adding (configuration editor).....1031
  - generating.....771, 1028
  - sample configuration.....1032
  - verifying SSL configuration.....1032
- standard software installation.....41
- standards documents
  - SNMP and MIBs.....1410
- start-time statement
  - accounting.....1993
  - usage guidelines.....1683
- startup messages, displaying.....387
- startup-alarm statement.....2028
  - usage guidelines.....1629
- stateless firewall filters
  - examples
    - blocking Telnet and SSH access.....1057
- statistics
  - BGP.....1825
  - interfaces.....1789
  - LSP.....1798
  - OSPF.....1824
  - performance monitoring.....1717
  - PPPoE.....1801
  - RIP.....1822
  - RPM, description.....1717
  - RPM, monitoring.....1736
  - RPM, verifying.....1724
- status
  - autoinstallation.....86
  - BGP.....1825
  - license key.....1146
  - OSPF interfaces.....1824
  - OSPF neighbors.....1824
  - RIP neighbors.....1822
- status command.....699
  - usage guidelines.....458, 504
- storage media.....30
  - device names
    - ACX Series, M Series, MX Series, T Series, TX Matrix, TX Matrix Plus, and JCS routers.....32
    - M Series, MX Series, T Series, TX Series, and TX Matrix Plus routers.....30
- storage space, freeing.....364, 374
- storing previous configurations.....525
- strings
  - help about.....448
- Structure of Management Information MIB.....1437
  - for EX Series.....1437
  - Junos OS for SRX Series devices, for.....1437
- Subscriber MIB.....1438
- super-user login class permissions.....795
- superuser login class permissions.....795
- support, technical See technical support
- switching platform
  - halting (J-Web).....219
  - rebooting (J-Web).....219
- symbol.....595
- syntax conventions.....lxiii
- sysContact object, MIB II.....1474, 1476
- sysDescription object, MIB II.....1475, 1476
- sysLocation object, MIB II.....1475, 1476
- syslog-subtag statement.....2028
  - usage guidelines.....1630
- sysName object, MIB II.....1477
- system.....823
  - backup-router statement.....199, 203
  - boot-message, logging.....192
  - information, obtaining.....206, 207
  - kernel messages, displaying.....194
  - login lockout.....291, 409, 1301, 1379
  - retry options.....823
  - storage, logging information.....196
- system access and access management
  - supported software standards.....2244
- system authentication
  - RADIUS
    - configuring.....1011
  - TACACS+.....1017
- System Configuration Statement Hierarchy.....1165



|                                                  |                  |                                             |      |
|--------------------------------------------------|------------------|---------------------------------------------|------|
| system contact, SNMP.....                        | 1474, 1476       | tacplus-server statement.....               | 1272 |
| system description, SNMP.....                    | 1475, 1476       | usage guidelines.....                       | 1017 |
| system location, SNMP.....                       | 1475, 1476, 2057 | tag statement.....                          | 2104 |
| system log messages                              |                  | SNMPv3                                      |      |
| event viewer.....                                | 1845             | usage guidelines.....                       | 1538 |
| System Log MIB.....                              | 1438             | usage guidelines.....                       | 1520 |
| system logs                                      |                  | tag-list statement.....                     | 2104 |
| file cleanup (CLI).....                          | 1135             | usage guidelines.....                       | 1524 |
| file cleanup (J-Web).....                        | 1134             | target-address statement.....               | 2105 |
| monitoring.....                                  | 1900             | usage guidelines.....                       | 1522 |
| system management                                |                  | target-parameters statement.....            | 2106 |
| displaying log and trace file contents.....      | 1900             | usage guidelines.....                       | 1526 |
| login classes.....                               | 795, 807         | targets statement.....                      | 2064 |
| template accounts.....                           | 810              | usage guidelines.....                       | 1491 |
| user accounts.....                               | 798, 807         | TCP                                         |      |
| user authentication.....                         | 804              | supported software standards.....           | 2278 |
| system memory                                    |                  | TCP RPM probes                              |      |
| M Series, MX Series, T Series, TX series, and TX |                  | CoS classification, destination interface   |      |
| Matrix Plus routers.....                         | 29               | requirement.....                            | 1725 |
| system name, SNMP.....                           | 1477             | CoS classification, use with caution.....   | 1725 |
| system overview                                  |                  | description.....                            | 1716 |
| software.....                                    | 17               | server port.....                            | 1733 |
| system services                                  |                  | setting.....                                | 1725 |
| outbound SSH.....                                | 1064             | verifying servers.....                      | 1727 |
| <b>T</b>                                         |                  | technical support                           |      |
| T1 ports                                         |                  | contacting JTAC.....                        | lxv  |
| alarm conditions and configuration               |                  | tee command.....                            | 732  |
| options.....                                     | 1705             | Telnet                                      |      |
| configuring alarms on.....                       | 1709             | accessing remote accounts (CLI).....        | 1062 |
| T3 interfaces                                    |                  | setting login retry limits.....             | 1052 |
| supported software standards.....                | 2252             | telnet command.....                         | 1062 |
| T3 ports                                         |                  | options.....                                | 1062 |
| alarm conditions and configuration               |                  | usage guidelines.....                       | 564  |
| options.....                                     | 1705             | Telnet session.....                         | 1062 |
| configuring alarms on.....                       | 1709             | temperature, environmental information..... | 192  |
| TACACS+                                          |                  | template accounts                           |      |
| authentication (configuration editor).....       | 1019             | description.....                            | 810  |
| order of user authentication (configuration      |                  | local accounts (configuration editor).....  | 810  |
| editor).....                                     | 1022             | remote accounts (configuration editor)..... | 810  |
| secret (configuration editor).....               | 1019             | temporary files                             |      |
| specifying for authentication.....               | 1022             | cleaning up (CLI).....                      | 1135 |
| supported software standards.....                | 2244             | cleaning up (J-Web).....                    | 1134 |
| TACACS+ authentication                           |                  | downloading (J-Web).....                    | 1137 |
| configuring.....                                 | 1017             | for packet capture.....                     | 1929 |
| tacplus.....                                     | 1270             | terminal screen                             |      |
| tacplus-options statement.....                   | 1271             | length, setting.....                        | 715  |
| usage guidelines.....                            | 1018             | width, setting.....                         | 716  |
|                                                  |                  | terminal type.....                          | 646  |
|                                                  |                  | setting.....                                | 717  |



- 
- tests See RPM
  - TFTP, for autoinstallation.....83, 90
  - threshold values, for RPM probes See RPM probes
  - time synchronization
    - supported software standards.....2245
  - timeout statement.....2082
    - authentication
      - usage guidelines, RADIUS.....1011
      - usage guidelines, TACACS+ .....1017
    - usage guidelines.....1534
  - timeout, user, setting.....712
  - timestamp, CLI output, setting.....718
  - timestamp-and-timezone statement.....1271
  - timestamps
    - for RPM probes See RPM probe timestamps
    - suppressing in packet headers, in captured packets.....1948
    - suppressing in packet headers, in traffic monitoring.....1943
  - Timing Feature Defect and Event Notification
    - MIB.....1436
  - top command.....700
    - usage guidelines.....458, 475
  - trace files
    - monitoring.....1900
    - multicast, monitoring.....1901
  - traceoptions (outbound-ssh).....1274
  - traceoptions statement.....701, 2065
    - datapath-debug.....2013
    - DHCP local server.....1276
    - EVPNs.....1994
    - resource monitoring.....2040
    - SNMP
      - usage guidelines.....1585
  - traceroute
    - CLI command.....1906
    - indications.....1904
    - J-Web tool.....1902
    - results.....1904
    - TTL increments.....1902
  - traceroute command.....1906
    - options.....1906
  - Traceroute MIB.....1438, 1569
  - traceroute monitor
    - CLI command.....1757
  - traceroute monitor command.....1757
    - options.....1757
    - results.....1758
  - Traceroute page
    - field summary.....1903
  - traceRouteHopsTable.....1574
  - tracing operations
    - SNMP.....1585
  - traffic
    - analyzing with packet capture.....1928
    - multicast, tracking.....1759
    - tracking with J-Web traceroute.....1902
  - transfer-interval statement
    - accounting.....1995
    - usage guidelines.....1683
  - trap groups, SNMP.....1491
  - trap notification for SNMP remote operations.....1561
  - trap-group statement.....2067
    - usage guidelines.....1491
  - trap-groups statement
    - usage guidelines.....1485
  - trap-options statement.....2068
    - usage guidelines.....1485, 1487
  - traps
    - spoofing.....2126
  - trim command.....732
  - Trivial File Transfer Protocol (TFTP), for autoinstallation.....83, 90
  - troubleshooting
    - applying CoS components on link services
      - interface.....1955
    - DNS name resolution in security policy.....1954
    - dropped packets on PVCs.....1964
    - J-Web access.....789
    - J-Web behavior.....789
    - jitter and latency on multilink bundles.....1957
    - LFI and load balancing on multilink bundles.....1957
    - packet capture for analysis.....1928
      - See also diagnosis; packet capture
    - root password recovery.....1953
    - router connectivity.....789
  - trusted-key statement.....1278
  - TTL (time to live)
    - default, in multicast path-tracking queries.....1759
    - increments, in traceroute packets.....1902
    - threshold, in multicast trace results.....1761
    - total, in multicast trace results.....1761
  - TX Matrix router
    - configuration groups.....615
    - configuration groups example.....619

|                         |      |
|-------------------------|------|
| type checking, CLI..... | 543  |
| type statement.....     | 2029 |
| usage guidelines.....   | 1520 |

## U

### UDP

|                                   |      |
|-----------------------------------|------|
| supported software standards..... | 2278 |
|-----------------------------------|------|

### UDP RPM probes

|                                                            |      |
|------------------------------------------------------------|------|
| CoS classification, destination interface requirement..... | 1725 |
| CoS classification, use with caution.....                  | 1725 |
| description.....                                           | 1716 |
| server port.....                                           | 1733 |
| setting.....                                               | 1725 |
| verifying servers.....                                     | 1727 |

|           |      |
|-----------|------|
| umd0..... | 1035 |
|-----------|------|

|                                           |     |
|-------------------------------------------|-----|
| unauthorized login class permissions..... | 795 |
|-------------------------------------------|-----|

|                                          |     |
|------------------------------------------|-----|
| unified in-service software upgrade..... | 122 |
|------------------------------------------|-----|

|                            |          |
|----------------------------|----------|
| UNIX operating system..... | 421, 422 |
|----------------------------|----------|

|                 |     |
|-----------------|-----|
| UNIX shell..... | 423 |
|-----------------|-----|

|                        |     |
|------------------------|-----|
| unprotect command..... | 702 |
|------------------------|-----|

|                       |     |
|-----------------------|-----|
| usage guidelines..... | 551 |
|-----------------------|-----|

### unprotecting configuration

|                       |     |
|-----------------------|-----|
| usage guidelines..... | 551 |
|-----------------------|-----|

|                 |     |
|-----------------|-----|
| up command..... | 703 |
|-----------------|-----|

|                       |          |
|-----------------------|----------|
| usage guidelines..... | 458, 475 |
|-----------------------|----------|

|                     |     |
|---------------------|-----|
| update command..... | 704 |
|---------------------|-----|

|                       |          |
|-----------------------|----------|
| usage guidelines..... | 458, 496 |
|-----------------------|----------|

|                                            |      |
|--------------------------------------------|------|
| update-router-advertisement statement..... | 1280 |
|--------------------------------------------|------|

|                                            |      |
|--------------------------------------------|------|
| update-server (dhcp-client) statement..... | 1280 |
|--------------------------------------------|------|

|                              |      |
|------------------------------|------|
| update-server statement..... | 1280 |
|------------------------------|------|

### updating

|                     |      |
|---------------------|------|
| licenses (CLI)..... | 1154 |
|---------------------|------|

|                                               |     |
|-----------------------------------------------|-----|
| updating configure private configuration..... | 496 |
|-----------------------------------------------|-----|

### upgrade Junos OS

|                         |     |
|-------------------------|-----|
| comparing software..... | 207 |
|-------------------------|-----|

|                                |     |
|--------------------------------|-----|
| upgrade, restarting after..... | 646 |
|--------------------------------|-----|

### upgraded FreeBSD

|               |     |
|---------------|-----|
| validate..... | 361 |
|---------------|-----|

### upgrades

|                  |     |
|------------------|-----|
| downloading..... | 150 |
|------------------|-----|

|                       |     |
|-----------------------|-----|
| installing (CLI)..... | 150 |
|-----------------------|-----|

|                              |         |
|------------------------------|---------|
| installing by uploading..... | 65, 150 |
|------------------------------|---------|

|                                    |         |
|------------------------------------|---------|
| installing from remote server..... | 65, 152 |
|------------------------------------|---------|

|                   |     |
|-------------------|-----|
| requirements..... | 147 |
|-------------------|-----|

|                                        |     |
|----------------------------------------|-----|
| upgrading or downgrading Junos OS..... | 116 |
|----------------------------------------|-----|

|                         |     |
|-------------------------|-----|
| upgrading software..... | 646 |
|-------------------------|-----|

|                 |     |
|-----------------|-----|
| performing..... | 334 |
|-----------------|-----|

### Upload package page

|                    |    |
|--------------------|----|
| field summary..... | 66 |
|--------------------|----|

### URLs

|                         |     |
|-------------------------|-----|
| software downloads..... | 150 |
|-------------------------|-----|

|                                   |     |
|-----------------------------------|-----|
| URLs, specifying in commands..... | 576 |
|-----------------------------------|-----|

|          |     |
|----------|-----|
| usb..... | 288 |
|----------|-----|

### USB modem connections

|                                           |      |
|-------------------------------------------|------|
| connecting dial-up modem at user end..... | 1049 |
|-------------------------------------------|------|

|                                                   |  |
|---------------------------------------------------|--|
| dialer interface <i>See</i> dialer interface, USB |  |
|---------------------------------------------------|--|

#### modem

|                                   |      |
|-----------------------------------|------|
| interface naming conventions..... | 1035 |
|-----------------------------------|------|

|                   |      |
|-------------------|------|
| requirements..... | 1038 |
|-------------------|------|

|                                |      |
|--------------------------------|------|
| USB modem interface types..... | 1035 |
|--------------------------------|------|

|                                  |      |
|----------------------------------|------|
| verifying dialer interfaces..... | 1045 |
|----------------------------------|------|

### USB modem interfaces

|                                                   |  |
|---------------------------------------------------|--|
| dialer interface <i>See</i> dialer interface, USB |  |
|---------------------------------------------------|--|

#### modem

### USB modems

|                  |      |
|------------------|------|
| AT commands..... | 1037 |
|------------------|------|

|                                            |      |
|--------------------------------------------|------|
| default modem initialization commands..... | 1037 |
|--------------------------------------------|------|

|                               |      |
|-------------------------------|------|
| initialization by device..... | 1037 |
|-------------------------------|------|

|                |      |
|----------------|------|
| resetting..... | 1050 |
|----------------|------|

|                              |      |
|------------------------------|------|
| use-interface statement..... | 1281 |
|------------------------------|------|

### user accounts

|                                     |  |
|-------------------------------------|--|
| authentication order (configuration |  |
|-------------------------------------|--|

|              |      |
|--------------|------|
| editor)..... | 1022 |
|--------------|------|

|                            |     |
|----------------------------|-----|
| configuration example..... | 432 |
|----------------------------|-----|

|               |     |
|---------------|-----|
| contents..... | 798 |
|---------------|-----|

|                                      |     |
|--------------------------------------|-----|
| creating (configuration editor)..... | 807 |
|--------------------------------------|-----|

|                      |     |
|----------------------|-----|
| for local users..... | 810 |
|----------------------|-----|

|                       |     |
|-----------------------|-----|
| for remote users..... | 810 |
|-----------------------|-----|

|                               |     |
|-------------------------------|-----|
| predefined login classes..... | 795 |
|-------------------------------|-----|

|                    |     |
|--------------------|-----|
| templates for..... | 810 |
|--------------------|-----|

*See also* template accounts

|                         |     |
|-------------------------|-----|
| user data, erasing..... | 377 |
|-------------------------|-----|

|                            |     |
|----------------------------|-----|
| user permission flags..... | 799 |
|----------------------------|-----|

### user roles

|              |     |
|--------------|-----|
| example..... | 815 |
|--------------|-----|

### user statement

|             |      |
|-------------|------|
| SNMPv3..... | 2107 |
|-------------|------|

|                            |     |
|----------------------------|-----|
| user timeout, setting..... | 712 |
|----------------------------|-----|

|                        |      |
|------------------------|------|
| user-id statement..... | 1282 |
|------------------------|------|

### username

|                  |     |
|------------------|-----|
| description..... | 798 |
|------------------|-----|

|                  |     |
|------------------|-----|
| specifying ..... | 807 |
|------------------|-----|

### users

|                        |          |
|------------------------|----------|
| access privileges..... | 795, 807 |
|------------------------|----------|

|                                   |  |
|-----------------------------------|--|
| accounts <i>See</i> user accounts |  |
|-----------------------------------|--|

|             |     |
|-------------|-----|
| adding..... | 807 |
|-------------|-----|

- CLI permissions, displaying.....723, 1345
  - editing configuration
    - displaying.....504
    - multiple simultaneous users.....511
  - login classes.....795, 807
  - of CLI, monitoring.....571
  - predefined login classes.....795
  - template accounts *See* template accounts
  - usernames.....798
  - usm statement.....2108
  - Utility MIB.....1438
- V**
- v3 statement.....2110
    - usage guidelines.....1500
  - vacm statement.....2112
    - usage guidelines.....1512
  - validate
    - upgraded FreeBSD.....361
  - validating software.....357
  - validating software compatibility.....47
  - var/log/mib2d file.....1585
  - var/log/snmpd file.....1585
  - variable statement.....2029
    - usage guidelines.....1630
  - variable-length string indexes.....1561
  - vendor-id statement.....1282
  - verification
    - active licenses.....260, 1156, 1158
    - alarm configurations.....1711
    - autoinstallation.....86
    - captured packets.....1932
    - destination path (J-Web).....1902
    - dialer interfaces.....1045
    - firewall filter for packet capture.....1937
    - host reachability (CLI).....1912
    - host reachability (J-Web).....1914
    - license usage.....261, 1156
    - licenses .....260, 1156, 1158
    - load balancing on the link services
      - interface.....1961
    - LSPs (J-Web).....1909
    - packet capture.....1932
    - packet encapsulation on link services
      - interface.....1960
    - RPM configuration.....1724
    - RPM probe servers.....1727, 1730
    - RPM statistics.....1724
    - secure access.....1032
    - tracing multicast paths.....1759
  - version
    - PPPoE, information about.....1801
  - version statement
    - SNMP.....2069
      - usage guidelines.....1491
  - version, license key.....1146
  - View Events page
    - field summary (filtering log messages).....1821
  - view statement
    - SNMP (associating with community).....2069
      - usage guidelines.....1479
    - SNMP (configuring MIB view).....2070
      - usage guidelines.....1496
  - views, MIB
    - SNMP.....1496, 1560
  - Virtual Chassis MIB.....1438
  - VLAN MIB.....1438
  - voice calls, not supported in dial-in .....1035
  - voice services
    - supported software standards.....2292
  - VPLS
    - supported software standards.....2296
  - VPLS MIBs.....1438
  - VPN Certificate Objects MIB.....1439
  - VPN MIB.....1439
  - vpn statement.....1283
  - VPNs
    - carrier-of-carriers
      - supported software standards.....2293
    - interprovider
      - supported software standards.....2293
    - Layer 2
      - supported software
        - standards.....2255, 2294
    - Layer 3
      - supported software standards.....2295
    - multicast
      - supported software standards.....2296
  - VPNs (virtual private networks), DHCP support on
    - interfaces.....1090
- W**
- Web access, secure *See* secure access
  - Web Filtering
    - verifying.....1866
  - web-management statement.....1285
  - wildcard characters.....622

|                           |      |
|---------------------------|------|
| wildcard command.....     | 707  |
| wildcard delete command   |      |
| usage guidelines.....     | 609  |
| wildcard names.....       | 633  |
| wildcard range command    |      |
| usage guidelines.....     | 485  |
| word history              |      |
| operational mode.....     | 454  |
| working directory         |      |
| current, setting.....     | 711  |
| displaying.....           | 724  |
| write-view statement..... | 2113 |
| usage guidelines.....     | 1516 |

## X

|                                   |     |
|-----------------------------------|-----|
| XML format                        |     |
| displaying command output in..... | 592 |

## Y

yellow alarms See minor alarms