



Junos[®] OS

Complete Software Guide for SRX Series Services Gateways, Release 12.3X48-D10 (Volume 1)

Release

12.3X48-D10



Modified: 2016-08-30

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.

Junos[®] OS Complete Software Guide for SRX Series Services Gateways, Release 12.3X48-D10 (Volume 1)
12.3X48-D10
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	liii
	Documentation and Release Notes	liii
	Supported Platforms	liii
	Using the Examples in This Manual	liii
	Merging a Full Example	liv
	Merging a Snippet	liv
	Documentation Conventions	lv
	Documentation Feedback	lvii
	Requesting Technical Support	lvii
	Self-Help Online Tools and Resources	lvii
	Opening a Case with JTAC	lviii
Part 1	Junos OS Getting Started Guide for Branch SRX Series	
Chapter 1	Overview	3
	Introduction to SRX Series Devices	3
	SRX Series Overview	3
Chapter 2	Setting Up a Branch SRX Series Services Gateway	5
	Understanding Factory Default Configuration Settings	5
	Understanding Factory Default Configuration Settings of an SRX210	5
	Default Configuration Topology	5
	Default Port Settings	6
	Default Settings for Interfaces, Zones, Policy, and NAT	7
	Default System Services	8
	Autoinstallation	8
	SRX210 Factory Default Settings—A Sample	8
	Configuring an SRX Series Device for the First Time	13
	Understanding Methods to Manage the Branch SRX Series	13
	Mandatory Settings to Configure the Branch SRX Series	14
	Connecting the Branch SRX Series Through the Console Port for the First Time	15
	Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network	16
	Configuring Internet Access for the Branch SRX Series	17
	Configuring a Network Time Protocol Server for the Branch SRX Series	18
	Validating the Branch SRX Series Configuration	19
	Verifying the Branch SRX Series Configuration	20
	Resetting the SRX Series Device	21
	Resetting the Branch SRX Series	21
	Resetting Your Branch SRX Series	21

Chapter 3	Configuring Basic SRX Series Features	23
	Configuring Security Zones and Policies for SRX Series	23
	Understanding Security Zones and Policies for SRX Series	23
	Zones	23
	Security Policy	24
	Example: Configuring Security Zones and Policies for SRX Series	24
	Configuring NAT for SRX Series	29
	Understanding NAT for SRX Series	29
	Example: Configuring Destination NAT for SRX Series	30
	Managing Licenses for SRX Series	35
	Updating Licenses for a Branch SRX Series	35
	Configuring UTM for Branch SRX Series	36
	Understanding Unified Threat Management for Branch SRX Series	37
	Example: Configuring Unified Threat Management for a Branch SRX Series	38
	Default UTM Policy for Branch SRX Series	42
	Default UTM Policy	42
	Predefined UTM Profile Configuration for Branch SRX Series	42
	Antispam	42
	Antivirus	42
	Web Filtering	44
	Configuring Intrusion Detection and Prevention for SRX Series	49
	Understanding Intrusion Detection and Prevention for SRX Series	49
	Example: Configuring Intrusion Detection and Prevention for SRX Series	50
	Understanding Stateful Firewall, IPsec VPN, and Chassis Cluster for Branch SRX Series	55
	Understanding Branch SRX Series Stateful Firewall Functionality	55
	Understanding IPsec VPN for SRX Series	56
	Understanding Chassis Cluster for SRX Series	56
Chapter 4	Configuration Statements and Operational Commands	57
	Configuration Statements	57
	Security Configuration Statement Hierarchy	57
	[edit security address-book] Hierarchy Level	58
	[edit security idp] Hierarchy Level	59
	[edit security ike] Hierarchy Level	69
	[edit security ipsec] Hierarchy Level	70
	[edit security nat] Hierarchy Level	72
	[edit security policies] Hierarchy Level	75
	[edit security utm] Hierarchy Level	80
	[edit security zones] Hierarchy Level	87
	Operational Commands	88
	request system license update	90
	show security flow session	91
	show security idp active-policy	97
	show security idp status	98
	show security nat destination summary	100
	show security policies	102
	show security utm session	110

	show security utm status	111
	show security zones	112
	show system license (View)	115
	show system services dhcp client	118
Part 2	Installation and Upgrade Guide for Security Devices	
Chapter 5	Junos Software and Hardware Overview	123
	Software Overview	123
	Junos OS Overview	123
	One Operating System	123
	One Modular Software Architecture	124
	Junos OS Editions	124
	FIPS 140-2 Security Compliance	125
	Junos OS Installation Packages	126
	Software Naming Convention	126
	Software Naming Convention for SRX Series Devices	126
	Software Package Information Security	127
	Junos OS Release Numbers	128
	Configuration Files	129
	Configuration File Selection Sequence	129
	Remote Storage of Configuration Files	130
	Hardware Overview	130
	Hardware Overview of SRX Series Services Gateways	130
	SRX Series Device Overview	130
	System Memory	131
	Storage Media	131
	Storage Media Names for SRX Series Devices	132
	Boot Sequence on SRX Series Devices	132
Chapter 6	Installing Junos OS Software	133
	Installation Overview	133
	Installation Type Overview	133
	Standard Installation	133
	Category Change Installation	134
	Recovery Installation	134
	Installation Categories on SRX Series Devices	134
	Understanding Download Manager for SRX Series Devices	135
	Overview	135
	Using Download Manager to Upgrade Junos OS	135
	Handling Errors	136
	Considerations	136
	Performing a Standard or Change Category Installation	137
	Checking the Current Configuration and Candidate Software	
	Compatibility	137
	Verifying PIC Combinations	137
	Determining the Junos OS Version	138
	Downloading Software	138
	Downloading Software with a Browser	139
	Downloading Software Using the Command-Line Interface	139

Downloading Software Packages from Juniper Networks	141
Backing Up the Current Installation on SRX Series Devices	141
Backing Up the Current Installation on SRX High-End Devices	141
Backing Up the Current Installation on Branch SRX Series Devices	142
Configuring External CompactFlash for SRX650 Devices	142
Connecting to the Console Port	143
Installing Software Using a USB Flash Drive	144
Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices	144
Installing Junos OS on SRX Series Devices Using a USB Flash Drive	146
Installing Software from the Boot Loader	147
Upgrading the Boot Loader on SRX Series Devices	147
Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server	148
Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device	150
Configuring Automatic Installation of Configuration Files	151
Autoinstallation Overview	151
Supported Autoinstallation Interfaces and Protocols	152
Typical Autoinstallation Process on a New Device	152
Configuring Autoinstallation on SRX Series Devices	154
Configuring Dual-Root Partitions for High Availability	156
Dual-Root Partitioning Scheme on SRX Series Devices	156
Boot Media and Boot Partition on SRX Series Devices	157
Important Features of the Dual-Root Partitioning Scheme	158
Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning	158
Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices	160
Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning	161
Example: Installing Junos OS on SRX Series Devices Using the Partition Option	162
Reinstalling the Single-Root Partition on SRX Series Devices	165

Upgrading Software	166
Upgrading Individual Software Packages	167
Understanding Junos OS Upgrades for SRX Series Devices	169
Understanding Junos OS Upgrades	169
Junos OS Upgrade Methods on the SRX Series Devices	169
Preparing Your SRX Series Device for Junos OS Upgrades	170
Secondary Storage Devices Available on SRX Series Devices	171
Verifying Available Disk Space on SRX Series Devices	171
Cleaning Up the System File Storage Space	172
Example: Installing Junos OS Upgrade Packages on SRX Series Devices . . .	173
Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server	175
Understanding BIOS Upgrades on SRX Series Devices	176
Understanding Manual BIOS Upgrade Using the Junos CLI	176
Understanding Auto BIOS Upgrade Methods on SRX Series Devices . .	177
Disabling Auto BIOS Upgrade on SRX Series Devices	178
Example: Downgrading Junos OS on SRX Series Devices	178
Booting a Device Using a System Snapshot	180
Example: Creating a Snapshot and Using It to Boot an SRX Series Device	181
Performing a Recovery Installation	183
Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices	184
Overview	184
How Autorecovery Works	184
How to Use Autorecovery	184
Data That Is Backed Up in an Autorecovery	185
Troubleshooting Alarms	185
Considerations	185
Saving a Rescue Configuration File	186
Restoring a Saved Configuration	187
Copy Saved Files to the Router	187
Load and Commit the Configuration File	188
Rebooting or Halting Software Processes on a Device	188
Restarting and Halting SRX Series Devices	189
Rebooting SRX Series Devices	189
Halting SRX Series Devices	190
Bringing Chassis Components Online and Offline on SRX Series Devices	192
Restarting the Chassis on SRX Series Devices	192
Configuring Administration User Accounts	193
Configure Administration User Accounts	193
Chapter 7 Installing and Managing Software Licenses	195
Software Licenses Overview	195
Junos OS Feature Licenses	195
License Enforcement	196

	Junos OS Feature License Keys	196
	License Key Components	197
	License Management Fields Summary	197
	Software Feature Licenses for SRX Series Devices	198
	Installing and Managing Licenses	208
	Working with License Keys for SRX Series Devices	209
	Generating a License Key	209
	Downloading License Keys	209
	Displaying License Keys in J-Web	209
	Saving License Keys	210
	Updating License Keys	210
	Example: Adding a New License Key	210
	Example: Deleting a License Key	213
Chapter 8	Configuration Statements and Operational Commands	217
	Configuration Statements	217
	System Configuration Statement Hierarchy	217
	auto-configuration	248
	auto-configuration (System)	249
	autoinstallation	251
	bootp	252
	commit	253
	configuration-servers	254
	interfaces (Autoinstallation)	255
	license	256
	usb	258
	usb-control	258
	Operational Commands	258
	request system autorecovery state	260
	request system download abort	262
	request system download clear	263
	request system download pause	264
	request system download resume	265
	request system download start	266
	request system firmware upgrade	267
	request system halt	268
	request system license update	270
	request system power-off	271
	request system snapshot (Maintenance)	273
	request system software abort in-service-upgrade (ICU)	276
	request system software add (Maintenance)	277
	request system software reboot	278
	request system software rollback (Maintenance)	279
	show chassis usb storage	280
	show system auto-snapshot	281
	show system autorecovery state	283
	show system download	285
	show system license (View)	287
	show system snapshot media	290

	show system storage (View SRX Series)	291
	show system storage partitions (View SRX Series)	293
	show version	295
Part 3	CLI User Guide	
Chapter 9	Overview	299
	Introduction to Junos OS CLI	299
	Key Features of the CLI	299
	Understanding the User Interfaces	301
	J-Web User Interface	301
	CLI	303
	Understanding the Junos OS CLI Modes, Commands, and Statement	
	Hierarchies	304
	Junos OS CLI Command Modes	304
	CLI Command Hierarchy	305
	Configuration Statement Hierarchy	305
	Moving Among Hierarchy Levels	306
	Other Tools to Configure and Monitor Devices Running Junos OS	307
	Commands and Configuration Statements for Junos-FIPS	307
Chapter 10	Getting Started: A Quick Tour of the CLI	309
	Getting Started with the Junos OS Command-Line Interface	309
	Switching Between Junos OS CLI Operational and Configuration Modes	311
	Configuring a User Account on a Device Running Junos OS	312
	Checking the Status of a Device Running Junos OS	314
	Example: Configuring a Routing Protocol	316
	Shortcut	317
	Longer Configuration	317
	Making Changes to a Routing Protocol Configuration	319
	Rolling Back Junos OS Configuration Changes	322
Chapter 11	Getting Online Help	325
	Getting Online Help from the Junos OS Command-Line Interface	325
	Getting Help About Commands	325
	Getting Help About a String in a Statement or Command	326
	Getting Help About Configuration Statements	327
	Getting Help About System Log Messages	327
	Junos OS CLI Online Help Features	327
	Help for Omitted Statements	327
	Using CLI Command Completion	328
	Using Command Completion in Configuration Mode	328
	Displaying Tips About CLI Commands	328
	Examples: Using Command Completion in Configuration Mode	329
	Displaying the Junos OS CLI Command and Word History	331
Chapter 12	Using Configuration Statements to Configure a Device	333
	Understanding the Junos Configuration Groups	334
	Configuration Groups Overview	334
	Inheritance Model	334

Configuring Configuration Groups	335
Understanding Junos OS CLI Configuration Mode	335
Configuration Mode Commands	336
Configuration Statements and Identifiers	337
Configuration Statement Hierarchy	339
Entering and Exiting the Junos OS CLI Configuration Mode	341
Forms of the configure Command	343
Using the configure exclusive Command	344
Example: Using the configure Command	345
Modifying the Junos OS Configuration	346
Adding Junos Configuration Statements and Identifiers	346
Deleting a Statement from a Junos Configuration	348
Example: Deleting a Statement from the Junos Configuration	349
Copying a Junos Statement in the Configuration	350
Example: Copying a Statement in the Junos Configuration	350
Issuing Relative Junos Configuration Mode Commands	351
Renaming an Identifier in a Junos Configuration	351
Example: Renaming an Identifier in a Junos Configuration	352
Inserting a New Identifier in a Junos Configuration	352
Example: Inserting a New Identifier in a Junos Configuration	352
Example: Using the Wildcard Command with the Range Option	354
Deactivating and Reactivating Statements and Identifiers in a Junos Configuration	358
Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration	359
Adding Comments in a Junos Configuration	360
Example: Including Comments in a Junos Configuration	361
Displaying the Current Junos OS Configuration	363
Example: Displaying the Current Junos OS Configuration	364
Displaying Additional Information About the Configuration	365
Displaying set Commands from the Junos OS Configuration	367
Example: Displaying set Commands from the Configuration	368
Example: Displaying Required set Commands at the Current Hierarchy Level	368
Example: Displaying set Commands with the match Option	369
Displaying Users Currently Editing the Configuration	369
Verifying a Junos Configuration	370
Chapter 13 Committing a Junos OS Configuration	371
Junos OS Commit Model for Router or Switch Configuration	371
Committing a Junos OS Configuration	372
Committing a Junos Configuration and Exiting Configuration Mode	375
Commit Operation When Multiple Users Configure the Software	375
Activating a Junos Configuration but Requiring Confirmation	376
Scheduling a Junos Commit Operation	377
Monitoring the Junos Commit Process	378
Adding a Comment to Describe the Committed Configuration	379
Backing Up the Committed Configuration on the Alternate Boot Drive	380

	Junos OS Batch Commits Overview	380
	Aggregation and Error Handling	381
	Example: Configuring Batch Commit Server Properties	381
Chapter 14	Managing Configurations	389
	Understanding How the Junos Configuration Is Stored	389
	Returning to the Most Recently Committed Junos Configuration	390
	Returning to a Previously Committed Junos OS Configuration	390
	Returning to a Configuration Prior to the One Most Recently Committed	390
	Displaying Previous Configurations	391
	Comparing Configuration Changes with a Prior Version	392
	Creating and Returning to a Rescue Configuration	393
	Saving a Configuration to a File	394
	Additional Details About Specifying Junos Statements and Identifiers	395
	Specifying Statements	395
	Performing CLI Type-Checking	397
	Loading a Configuration from a File	398
	Examples: Loading a Configuration from a File	401
	Creating and Returning to a Rescue Configuration	403
	Example: Protecting the Junos OS Configuration from Modification or	
	Deletion	404
	Synchronizing Routing Engines	410
Chapter 15	Using Operational Commands to Monitor a Device	413
	Overview of Junos OS CLI Operational Mode Commands	413
	CLI Command Categories	413
	Commonly Used Operational Mode Commands	415
	Junos OS Operational Mode Commands That Combine Other Commands	416
	Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS	
	Operational Commands	417
	Controlling the Scope of an Operational Mode Command	418
	Operational Mode Commands on a TX Matrix Router or TX Matrix Plus	
	Router	419
	Examples of Routing Matrix Command Options	419
	Monitoring Who Uses the Junos OS CLI	421
	Interface Naming Conventions Used in the Junos OS Operational	
	Commands	422
	Physical Part of an Interface Name	422
	Logical Part of an Interface Name	423
	Channel Identifier Part of an Interface Name	423
	Viewing Files and Directories on a Device Running Junos OS	423
	Directories on the Router or Switch	424
	Listing Files and Directories	424
	Specifying Filenames and URLs	426
	Displaying Junos OS Information	427
	Managing Programs and Processes Using Junos OS Operational Mode	
	Commands	429
	Showing Software Processes	430
	Restarting a Junos OS Process	431
	Stopping the Junos OS	432

	Rebooting the Junos OS	433
	Using the Junos OS CLI Comment Character # for Operational Mode Commands	434
	Example: Using Comments in Junos OS Operational Mode Commands	434
Chapter 16	Filtering Command Output	437
	Using the Pipe () Symbol to Filter Junos Command Output	437
	Using Regular Expressions with the Pipe () Symbol to Filter Junos Command Output	438
	Pipe () Filter Functions in the Junos OS command-line interface	439
	Comparing Configurations	439
	Counting the Number of Lines of Output	441
	Displaying Output in XML Tag Format	441
	Displaying the RPC tags for a Command	441
	Ignoring Output That Does Not Match a Regular Expression	441
	Displaying Output from the First Match of a Regular Expression	442
	Retaining Output After the Last Screen	442
	Displaying Output Beginning with the Last Entries	442
	Displaying Output That Matches a Regular Expression	443
	Preventing Output from Being Paginated	443
	Sending Command Output to Other Users	443
	Resolving IP Addresses	444
	Saving Output to a File	444
	Trimming Output by Specifying the Starting Column	444
Chapter 17	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	447
	Using Keyboard Sequences to Move Around and Edit the Junos OS CLI	447
	Using Wildcard Characters in Interface Names	449
	Common Regular Expressions to Use with the replace Command	450
	Using Global Replace in a Junos Configuration	451
	Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference	452
	Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name	453
	Example: Using Global Replace in a Junos Configuration—Using the upto Option	454
	Using Regular Expressions to Delete Related Items from a Junos Configuration	455
Chapter 18	Using Configuration Groups to Quickly Configure Devices	457
	Creating a Junos Configuration Group	457
	Applying a Junos Configuration Group	459
	Example: Configuring and Applying Junos Configuration Groups	460
	Example: Creating and Applying Configuration Groups on a TX Matrix Router . .	462
	Disabling Inheritance of a Junos OS Configuration Group	463
	Using Wildcards with Configuration Groups	465
	Example : Configuring Sets of Statements with Configuration Groups	468
	Example: Configuring Interfaces Using Junos OS Configuration Groups	469
	Example: Configuring a Consistent IP Address for the Management Interface . .	471
	Example: Configuring Peer Entities	472

	Establishing Regional Configurations	474
	Selecting Wildcard Names	475
	Example: Referencing the Preset Statement From the Junos defaults Group	477
	Example: Viewing Default Statements That Have Been Applied to the Configuration	478
	Using Conditions to Apply Configuration Groups Overview	478
	Example: Configuring Conditions for Applying Configuration Groups	478
	Using Junos OS Defaults Groups	481
Chapter 19	Controlling the CLI Environment	483
	Controlling the Junos OS CLI Environment	483
	Setting the Terminal Type	484
	Setting the CLI Prompt	484
	Setting the CLI Directory	484
	Setting the CLI Timestamp	484
	Setting the Idle Timeout	484
	Setting the CLI to Prompt After a Software Upgrade	484
	Setting Command Completion	485
	Displaying CLI Settings	485
	Example: Controlling the CLI Environment	485
	Setting the Junos OS CLI Screen Length and Width	486
	Setting the Screen Length	486
	Setting the Screen Width	486
	Understanding the Screen Length and Width Settings	486
Chapter 20	Junos OS Configuration Statements and Commands	489
	apply-groups	490
	apply-groups-except	490
	commit-interval (Batch Commits)	491
	days-to-keep-error-logs (Batch Commits)	491
	deactivate	492
	delete	493
	edit	494
	exit	495
	groups	496
	help	498
	insert	499
	load	500
	maximum-aggregate-pool (Batch Commits)	501
	maximum-entries (Batch Commits)	502
	protect	503
	quit	504
	rename	505
	replace	506
	rollback	507
	run	508
	save	509
	server (Batch Commits)	510
	set	511
	status	512

	top	513
	traceoptions (Batch Commits)	514
	unprotect	515
	up	516
	update	517
	when	518
	wildcard delete	519
Chapter 21	Junos OS CLI Environment Commands	521
	set cli complete-on-space	522
	set cli directory	523
	set cli idle-timeout	524
	set cli prompt	525
	set cli restart-on-upgrade	526
	set cli screen-length	527
	set cli screen-width	528
	set cli terminal	529
	set cli timestamp	530
	set date	531
	show cli	532
	show cli authorization	534
	show cli directory	535
	show cli history	536
Chapter 22	Junos OS CLI Operational Mode Commands	537
	activate	538
	annotate	539
	commit	540
	configure	543
	copy	545
	file	546
	help	547
	(pipe)	548
	request	550
	restart	552
	set	562
	show	563
	show configuration	564
	show display inheritance	567
	show display omit	568
	show display set	569
	show display set relative	570
	show groups junos-defaults	571
	show system commit	572

Part 4	J-Web User Guide	
Chapter 23	Overview	577
	Introduction to J-Web	577
	J-Web Overview	577
	Understanding the J-Web User Interface	578
	Understanding the User Interfaces	578
	J-Web User Interface	579
	CLI	580
	Starting the J-Web User Interface	581
	Understanding the J-Web Interface Layout	583
	J-Web Commit Options Guidelines	584
	Getting Help in the J-Web User Interface	585
	Establishing J-Web Sessions	586
	J-Web Layout	587
	Top Pane Elements	587
	Main Pane Elements	588
	Side Pane Elements	589
	Navigating the J-Web Interface	589
	Navigating the J-Web Configuration Editor	590
	Getting J-Web Help	590
	Understanding Configuration Tools in J-Web	591
	Configuration Task Overview	591
	Point and Click CLI (J-Web Configuration Editor)	593
	CLI Viewer (View Configuration Text)	595
	CLI Editor (Edit Configuration Text)	597
	CLI Terminal Requirements	598
	Starting the CLI Terminal	598
	Using the CLI Terminal	599
Chapter 24	Configuring a Device Using J-Web	603
	Installing and Starting J-Web	603
	J-Web Software Requirements	603
	Installing the J-Web Software	603
	Starting the J-Web Interface	604
	Configuring Secure Web Access to a Device	605
	Secure Web Access Overview	605
	Generating SSL Certificates	605
	Configuring Secure Web Access	606
	Configuring a Device Using J-Web	608
	Configuring Basic Settings	609
	Editing and Committing a Junos OS Configuration	612
	J-Web Configuration Tasks	612
	Editing a Configuration	613
	Committing a Configuration	615
	Discarding Parts of a Candidate Configuration	616
	Accounting Options	616

Chapter 25	Administering a Device Using J-Web	619
	Managing Configurations and Files on a Device	619
	Displaying Configuration History	619
	Displaying Users Editing the Configuration	621
	Loading a Previous Configuration File	622
	Downloading a Configuration File	623
	Comparing Configuration Files	623
	Upload Configuration File	624
	Using Files	625
	Managing Software on a Device	626
	Sample Task—Manage Snapshots	626
	Using Reboot	627
	Configuring and Viewing Alarms on a Device	627
	Using Alarms	628
	View Alarms	628
	Active Alarms Information	628
	Alarm Severity	629
	Displaying Alarm Descriptions	629
	Sample Task—Viewing and Filtering Alarms	629
	Viewing and Filtering System Log Events on a Device	630
	Using View Events	630
	Viewing Events	631
	View Events	631
	Understanding Severity Levels	632
	Using Filters	632
	Using Regular Expressions	634
	Sample Task—Filtering and Viewing Events	635
	Monitoring a Device	636
	Monitor Task Overview	636
	Class of Service	637
	Interfaces	637
	MPLS	638
	RPM	639
	Routing	640
	Security	641
	Firewall	641
	IPsec	642
	NAT	642
	Service Sets	643
	Services	643
	System View	644
	System Information	644
	Chassis Information	644
	Process Details	645
	FEB Redundancy (M120 Routing Platforms Only)	645
	Sample Task—Monitoring Interfaces	645
	Sample Task—Monitoring Route Information	647

	Managing J-Web Sessions and Users	649
	Setting J-Web Session Limits	649
	Terminating J-Web Sessions	649
	Viewing Current Users	649
Chapter 26	Troubleshooting	651
	Troubleshooting the J-Web User Interface	651
	Lost Router Connectivity	651
	Unpredictable J-Web Behavior	651
	No J-Web Access	652
	Troubleshooting System Log Events	652
	Troubleshooting Events	652
	Troubleshooting the Network	653
	Using Ping Host	653
	Using Ping MPLS	654
	Using Traceroute	656
	Using Packet Capture	656
	Sample Task—Ping Host	657
Part 5	Administration Guide for Security Devices	
Chapter 27	User Access and Authentication	663
	User Access and Authentication Overview	663
	Understanding Login Classes	663
	Permission Bits	664
	Denying or Allowing Individual Commands	666
	Understanding User Accounts	667
	Understanding Junos OS Access Privilege Levels	669
	Junos OS Login Class Permission Flags	669
	Allowing or Denying Individual Commands for Junos OS Login Classes	672
	Understanding User Authentication Methods	673
	Configuring Junos OS User Accounts	674
	Example: Configuring New Users	674
	Understanding Template Accounts	677
	Example: Creating Template Accounts	677
	Understanding Administrative Roles	680
	Example: Configuring Administrative Roles	682
	Handling Authorization Failure	689
	Example: Configuring System Retry Options	690

Configuring User Access Privileges	694
Configuring Access Privilege Levels	694
Example: Configuring Access Privilege Levels	695
Specifying Access Privileges for Junos OS Operational Mode	
Commands	695
Example: Configuring Access Privileges for Operational Mode	
Commands	697
Specifying Access Privileges for Junos OS Configuration Mode	
Hierarchies	697
Example: Specifying Access Privileges Using	
allow/deny-configuration-regexps Statements	698
Permissions Flags for User Access Privileges	702
Access Privilege User Permission Flags Overview	703
access	705
access-control	706
admin	706
admin-control	707
all-control	708
clear	708
configure	742
control	742
field	742
firewall	743
firewall-control	743
floppy	744
flow-tap	744
flow-tap-control	745
flow-tap-operation	745
idp-profiler-operation	746
interface	746
interface-control	747
maintenance	748
network	754
pgcp-session-mirroring	755
pgcp-session-mirroring-control	756
reset	756
rollback	757
routing	757
routing-control	761
secret	765
secret-control	766
security	767
security-control	771
shell	774
snmp	774
system	775
system-control	777
trace	778
trace-control	783

	view	788
	view-configuration	851
	Configuring Authentication Methods	851
	Configuring RADIUS Server Authentication	851
	Example: Configuring a RADIUS Server for System Authentication	855
	Configuring TACACS+ Authentication	857
	Configuring TACACS+ Server Details	857
	Specifying a Source Address for the Junos OS to Access External TACACS+ Servers	858
	Configuring the Same Authentication Service for Multiple TACACS+ Servers	858
	Configuring Juniper Networks Vendor-Specific TACACS+ Attributes	859
	Example: Configuring a TACACS+ Server for System Authentication	859
	Example: Configuring Authentication Order	862
Chapter 28	Configuring Remote Access to an SRX Series Appliances	865
	Configuring Secure Web Access	865
	Secure Web Access Overview	865
	Generating an SSL Certificate Using the openssl Command	866
	Generating a Self-Signed SSL Certificate	866
	Manually Generating Self-Signed SSL Certificates	867
	Configuring Device Addresses	868
	Enabling Access Services	868
	Example: Configuring Secure Web Access	869
	Adding, Editing, and Deleting Certificates on the Device	871
	Setting up USB Modems for Remote Management	872
	USB Modem Interface Overview	872
	USB Modem Interfaces	873
	Dialer Interface Rules	873
	How the Device Initializes USB Modems	874
	USB Modem Configuration Overview	875
	Example: Configuring a USB Modem Interface	877
	Example: Configuring a Dialer Interface	879
	Example: Configuring a Dialer Interface for USB Modem Dial-In	883
	Configuring a Dial-Up Modem Connection Remotely	885
	Connecting to the Device Remotely	886
	Modifying USB Modem Initialization Commands	886
	Resetting USB Modems	887
	Configuring Telnet and SSH Access to an SRX Series Appliance	887
	Securing the Console Port Configuration Overview	888
	Configuring Password Retry Limits for Telnet and SSH Access	889
	Configuring Reverse Telnet and Reverse SSH	890
	Example: Controlling Management Access on SRX Series Devices	890
	Example: Configuring a Filter to Block Telnet and SSH Access	893
	The telnet Command	898
	The ssh Command	899
	Configuring Outbound SSH Service	900
	Configuring the Device Identifier for Outbound SSH Connections	901
	Sending the Public SSH Host Key to the Outbound SSH Client	901

	Configuring Keepalive Messages for Outbound SSH Connections	902
	Configuring a New Outbound SSH Connection	902
	Configuring the Outbound SSH Client to Accept NETCONF as an Available Service	903
	Configuring Outbound SSH Clients	903
Chapter 29	Configuring DNS	905
	Configuring DNS Server Caching, DNSSEC, and DNS Proxy	905
	DNS Overview	905
	DNS Components	905
	DNS Server Caching	906
	Example: Configuring the TTL Value for DNS Server Caching	906
	DNSSEC Overview	907
	Example: Configuring DNSSEC	907
	Example: Configuring Keys for DNSSEC	908
	Example: Configuring Secure Domains and Trusted Keys for DNSSEC	908
	DNS Proxy Overview	910
	DNS Proxy Cache	910
	DNS Proxy with Split DNS	910
	Dynamic Domain Name System Client	912
	Configuring the Device as a DNS Proxy	914
Chapter 30	Configuring DHCP Access Service for IP Address Management	917
	Understanding DHCP Services	917
	DHCP Overview	917
	DHCP Local Server	917
	DHCP Client	918
	DHCP Relay Agent	919
	DHCP Client, DHCP Relay Agent, and DHCP Local Servers	919
	Considerations	920
	DHCP Server, Client, and Relay Agent Overview	920
	DHCP Settings and Restrictions Overview	921
	Propagation of TCP/IP Settings for DHCP	921
	DHCP Conflict Detection and Resolution	922
	DHCP Interface Restrictions	922
	Configuring a DHCP Local Server	922
	Understanding DHCP Server Operation	922
	DHCP Options	923
	Compatibility with Autoinstallation	923
	Chassis Cluster Support	923
	DHCP Server Configuration Overview	924
	Minimum DHCP Local Server Configuration	925
	Configuring Address-Assignment Pools	926
	Configuring an Address-Assignment Pool Name and Addresses	926
	Configuring a Named Address Range for Dynamic Address Assignment . . .	927
	Configuring Static Address Assignments	927
	Enabling TCP/IP Propagation on a DHCP Local Server	928
	Verifying and Managing DHCP Local Server Configuration	928
	Example: Configuring the Device as a DHCP Server	929

Configuring a DHCP Client	935
Understanding DHCP Client Operation	935
Minimum DHCP Client Configuration	935
Configuring DHCP Client-Specific Attributes for Address-Assignment Pools	936
Configuring Optional DHCP Client Attributes	937
Verifying and Managing DHCP Client Configuration	937
Example: Configuring the Device as a DHCP Client	938
Configuring a DHCP Relay Agent	942
Understanding DHCP Relay Agent Operation	943
Minimum DHCP Relay Agent Configuration	943
Verifying and Managing DHCP Relay Configuration	944
Example: Configuring the Device as a BOOTP or DHCP Relay Agent	944
Configuring a DHCPv6 Local Server	949
DHCPv6 Server Overview	949
Creating a Security Policy for DHCPv6	950
Example: Configuring DHCPv6 Server Options	950
Example: Configuring an Address-Assignment Pool	953
Configuring a Named Address Range for Dynamic Address Assignment	955
Configuring Address-Assignment Pool Linking	956
Configuring DHCP Client-Specific Attributes	956
Configuring an Address-Assignment Pool for Router Advertisement	957
Understanding DHCPv6 Client and Server Identification	958
Configuring a DHCPv6 Client	958
DHCPv6 Client Overview	959
Minimum DHCPv6 Client Configuration	960
Configuring Optional DHCPv6 Client Attributes	961
Configuring Nontemporary Address Assignment	962
Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation	962
Configuring Auto-Prefix Delegation	963
Configuring the DHCPv6 Client Rapid Commit Option	964
Configuring a DHCPv6 Client in Autoconfig Mode	964
Configuring TCP/IP Propagation on a DHCPv6 Client	965
Configuring DHCP in Chassis Cluster Mode	965
Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode	965
Example: Configuring the Device as a DHCP Client in Chassis Cluster Mode	970
Chapter 31 Managing System Files	977
Performing File Management Tasks	977
File Management Overview	977
Decrypting Configuration Files	978
Encrypting Configuration Files	978
Modifying the Encryption Key	979
Cleaning Up Files	980
Cleaning Up Files with the CLI	981
Deleting Files	982

	Deleting the Backup Software Image	982
	Downloading Files	983
	Configuring RADIUS System Accounting	983
	Configuring Auditing of User Events on a RADIUS Server	984
	Specifying RADIUS Server Accounting and Auditing Events	984
	Configuring RADIUS Server Accounting	984
	Managing Accounting Files	986
Chapter 32	Working with Junos OS Licenses	989
	Managing Junos OS Licenses	989
	Junos OS Feature License Keys	989
	License Key Components	989
	License Management Fields Summary	990
	Software Feature Licenses for SRX Series Devices	991
	Displaying License Keys in J-Web	1000
	Downloading License Keys	1001
	Generating a License Key	1001
	Saving License Keys	1002
	Updating License Keys	1003
	Example: Adding a New License Key	1003
	Example: Deleting a License Key	1006
Chapter 33	Configuration Statements and Operational Commands	1009
	Configuration Statements	1009
	[edit security certificates] Hierarchy Level	1012
	[edit security ssh-known-hosts] Hierarchy Level	1012
	Interfaces Configuration Statement Hierarchy	1012
	Groups Configuration Statement Hierarchy	1028
	System Configuration Statement Hierarchy	1028
	address-assignment (Access)	1060
	address-pool (Access)	1063
	allow-configuration	1064
	allow-configuration-regexps	1065
	authentication-key	1066
	authentication-order	1067
	boot-server (NTP)	1068
	broadcast	1069
	broadcast-client	1070
	ciphers	1071
	connection-limit	1072
	client-ia-type	1073
	client-identifier (dhcp-client)	1073
	client-identifier (dhcpv6-client)	1074
	client-list-name (SNMP)	1074
	client-type	1075
	deny-configuration	1075
	deny-configuration-regexps	1076
	destination (Accounting)	1077
	dhcp-attributes (Access IPv4 Address Pools)	1078
	dhcp-attributes (Access IPv6 Address Pools)	1080

dhcp-client	1081
dhcp-local-server (System Services)	1082
dhcpv6 (System Services)	1086
dhcpv6-client	1089
disable (System Services)	1090
dlv	1090
family (Security Forwarding Options)	1091
file (System Logging)	1092
forwarding-options (Security)	1095
group (System Services DHCP)	1096
host (SSH Known Hosts)	1099
hostkey-algorithm	1100
interface (System Services DHCP)	1101
interfaces (ARP)	1102
interfaces (Security Zones)	1103
interface-traceoptions (System Services DHCP)	1104
internet-options	1106
kernel-replication (System)	1107
lease-time (dhcp-client)	1107
location	1108
lockout-period	1109
macs	1110
max-pre-authentication-packets	1111
multicast-client	1111
name-server (Access)	1112
neighbor-discovery-router-advertisement (Access)	1112
ntp	1113
outbound-ssh	1114
overrides (System Services DHCP)	1116
peer (NTP)	1117
prefix	1118
proflerd	1119
protocol-version	1119
proxy	1120
radius-options	1121
radius-server	1122
rapid-commit	1123
reconfigure (System Services DHCP)	1124
req-option	1125
retransmission-attempt (dhcp-client)	1126
retransmission-attempt (dhcpv6-client)	1126
retransmission-interval (dhcp-client)	1127
root-authentication	1128
single-connection	1129
server (NTP)	1130
server-address (dhcp-client)	1131
services (System Services)	1132
source-address (NTP, RADIUS, System Logging, or TACACS+)	1137
ssh-known-hosts	1138

static-subscribers	1139
statistics-service	1139
subscriber-management	1140
subscriber-management-helper	1141
tacplus	1142
tacplus-options	1143
tacplus-server	1144
traceoptions (Outbound SSH)	1146
traceoptions (System Services DHCP)	1148
trusted-key	1150
uac-service	1151
update-router-advertisement	1152
update-server (dhcp-client)	1152
update-server (dhcpv6-client)	1152
usb-control	1153
use-interface	1153
user-id	1154
vendor-id	1154
vpn (Forwarding Options)	1155
watchdog	1155
web-management	1156
web-management (System Services)	1157
Operational Commands	1160
clear dhcp client binding	1163
clear dhcp client statistics	1164
clear dhcp relay binding	1165
clear dhcp relay statistics	1166
clear dhcp server binding	1167
clear dhcp server statistics	1168
clear dhcpv6 client binding	1169
clear dhcpv6 client statistics	1170
clear dhcpv6 server binding (Local Server)	1171
clear dhcpv6 server statistics (Local Server)	1172
clear system login logout	1173
file archive	1174
file checksum md5	1176
file checksum sha1	1177
file checksum sha-256	1178
file compare	1179
file copy	1182
file delete	1184
file list	1185
file rename	1186
file show	1187
request dhcp client renew	1188
request dhcpv6 client renew	1189
request system autorecovery state	1190
request system download abort	1192
request system download clear	1193

request system download pause	1194
request system download resume	1195
request system download start	1196
request system firmware upgrade	1197
request system license update	1198
request system power-off fpc	1199
request system services dhcp	1200
request system snapshot (Maintenance)	1201
request system software abort in-service-upgrade (ICU)	1204
request system software add (Maintenance)	1205
request system software reboot	1206
request system software rollback (Maintenance)	1207
request support information	1208
request system zeroize	1222
restart (Reset)	1224
Restart Commands Overview	1229
show chassis routing-engine (View)	1230
show cli authorization	1233
show dhcp client binding	1234
show dhcp client statistics	1237
show dhcp relay binding	1239
show dhcp relay statistics	1241
show dhcp server binding	1243
show dhcp server statistics	1245
show dhcpv6 client binding	1247
show dhcpv6 client statistics	1249
show dhcpv6 server binding (View)	1251
show dhcpv6 server statistics (View)	1255
show firewall (View)	1258
show system autorecovery state	1260
show system directory-usage	1262
show system download	1264
show system license (View)	1266
show system login lockout	1269
show system services dhcp client	1270
show system services dhcp relay-statistics	1273
show system snapshot media	1275
show system storage (View SRX Series)	1276
show system storage partitions (View SRX Series)	1278

Part 6	Monitoring and Troubleshooting Library for Security Devices
Chapter 34	Network Monitoring and Troubleshooting Guide for Security Devices . . 1283
	Overview 1283
	Introduction to Network Monitoring 1283
	Monitoring Overview 1283
	Diagnostic Tools Overview 1284
	Accounting Options, Source Class Usage, and Destination Class Usage
	Overview 1287
	Accounting Options Overview 1287
	Understanding Source Class Usage and Destination Class Usage
	Options 1288
	Gathering Statistics for Accounting Purposes 1289
	Accounting Options Configuration 1289
	Configuring Accounting-Data Log Files 1292
	Configuring the Interface Profile 1295
	Configuring the Filter Profile 1297
	Example: Configuring a Filter Profile 1299
	Example: Configuring Interface-Specific Firewall Counters
	and Filter Profiles 1300
	Configuring SCU or DCU 1301
	Configuring SCU on a Virtual Loopback Tunnel Interface 1303
	Configuring Class Usage Profiles 1304
	Configuring the MIB Profile 1307
	Configuring the Routing Engine Profile 1308
	Configuring Monitoring Options 1310
	Configuring Interface Alarms 1310
	Alarm Overview 1310
	Example: Configuring Interface Alarms 1316
	Monitoring Active Alarms on a Device 1318
	Monitoring Alarms 1319
	Using RPM to Measure Network Performance 1321
	RPM Overview 1321
	RPM Support for VPN Routing and Forwarding 1325
	Example: Configuring Basic RPM Probes 1325
	Example: Configuring RPM Using TCP and UDP Probes 1329
	Example: Configuring RPM Probes for BGP Monitoring 1332
	Directing RPM Probes to Select BGP Devices 1334
	Configuring RPM Timestamping 1335
	Tuning RPM Probes 1336
	RPM Configuration Options 1337
	Monitoring RPM Probes 1340
	Configuring IP Monitoring 1344
	IP Monitoring Overview 1344
	Understanding IP Monitoring Test Parameters 1345
	Example: Configuring IP Monitoring on Branch SRX Series Devices . . 1346

Understanding IP Monitoring Through Redundant Ethernet Interface	
Link Aggregation Groups	1348
Example: Configuring IP Monitoring on High-End SRX Series	
Devices	1349
Example: Configuring Chassis Cluster Redundancy Group IP Address	
Monitoring	1354
Monitoring Common Security Features	1357
Displaying Real-Time Information from Device to Host	1358
Displaying Multicast Path Information	1358
Displaying Real-Time Monitoring Information	1360
Monitoring Application Layer Gateways Features	1362
Monitoring H.323 ALG Information	1363
Monitoring MGCP ALGs	1364
Monitoring SCCP ALGs	1367
Monitoring SIP ALGs	1369
Monitoring Voice ALG H.323	1373
Monitoring Voice ALG MGCP	1375
Monitoring Voice ALG SCCP	1378
Monitoring Voice ALG SIP	1381
Monitoring Voice ALG Summary	1386
Monitoring Class-of-Service	1387
Monitoring Class-of-Service Performance	1387
Monitoring CoS Classifiers	1393
Monitoring Interfaces and Switching Functions	1394
Displaying Real-Time Interface Information	1395
Monitoring Address Pools	1397
Monitoring Ethernet Switching	1398
Monitoring GVRP	1399
Monitoring Interfaces	1400
Monitoring MPLS Traffic Engineering Information	1401
Monitoring PPP	1406
Monitoring PPPoE	1407
Monitoring Spanning Tree	1410
Monitoring the WAN Acceleration Interface	1411
Monitoring NAT	1411
Monitoring NAT	1412
Monitoring Security Policies	1422
Monitoring Policy Statistics	1422
Monitoring Routing Information	1423
Monitoring Security Events by Policy	1430
Monitoring Security Features	1432
Monitoring Events, Services and System	1447
Monitoring DHCP Client Bindings	1447
Monitoring Events	1447
Monitoring the System	1450
Monitoring Unified Threat Management Features	1455
Monitoring Antivirus Scan Engine Status	1455
Monitoring Antivirus Scan Results	1456
Monitoring Antivirus Session Status	1458

Monitoring Content Filtering Configurations	1459
Monitoring Reports	1459
Monitoring Web Filtering Configurations	1466
Monitoring VPNs	1466
Monitoring VPNs	1467
Troubleshooting	1477
Configuring Data Path Debugging and Trace Options	1477
Understanding Data Path Debugging for SRX Series Devices	1477
Debugging the Data Path (CLI Procedure)	1479
Example: Configuring End-to-End Debugging on a High-End SRX Series Device	1479
Understanding Security Debugging Using Trace Options	1483
Setting Security Trace Options (CLI Procedure)	1483
Displaying Log and Trace Files	1485
Displaying Output for Security Trace Options	1485
Displaying Multicast Trace Operations	1486
Using the J-Web Traceroute Tool	1486
J-Web Traceroute Results and Output Summary	1488
Understanding Flow Debugging Using Trace Options	1489
Setting Flow Debugging Trace Options (CLI Procedure)	1489
Displaying a List of Devices	1490
Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits	1491
MPLS Connection Checking Overview	1492
Configuring Ping MPLS	1494
Using the ping Command	1494
Using the J-Web Ping Host Tool	1496
J-Web Ping Host Results and Output Summary	1498
Using the J-Web Ping MPLS Tool	1499
J-Web Ping MPLS Results and Output Summary	1502
Pinging Layer 2 Circuits	1503
Pinging Layer 2 VPNs	1504
Pinging Layer 3 VPNs	1506
Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs	1507
Using Packet Capture to Analyze Network Traffic	1508
Packet Capture Overview	1508
Example: Enabling Packet Capture on a Device	1511
Example: Configuring Packet Capture on an Interface	1514
Example: Configuring a Firewall Filter for Packet Capture	1516
Example: Configuring Packet Capture for Datapath Debugging	1518
Disabling Packet Capture	1521
Deleting Packet Capture Files	1521
Changing Encapsulation on Interfaces with Packet Capture Configured	1522
Displaying Packet Headers	1523
Using the J-Web Packet Capture Tool	1527
J-Web Packet Capture Results and Output Summary	1530

Troubleshooting Security Devices	1531
Recovering the Root Password for SRX Series Devices	1532
Troubleshooting Access Manager Client-Side Problems	1533
Troubleshooting DNS Name Resolution in Logical System Security Policies (Master Administrators Only)	1533
Troubleshooting the Link Services Interface	1534
Troubleshooting Security Policies	1543
Troubleshooting ISSU-Related Problems Using Log Error Messages ..	1545
Configuration Statements and Operational Commands	1547
Configuration Statements	1548
Chassis Configuration Statement Hierarchy	1549
Accounting-Options Configuration Statement Hierarchy	1552
[edit security] Hierarchy Level	1554
[edit security alarms] Hierarchy Level	1555
[edit security datapath-debug] Hierarchy Level	1556
[edit security traceoptions] Hierarchy Level	1557
accounting-options	1557
action-profile	1558
archive-sites	1559
capture-file (Security)	1560
class-usage-profile	1561
cluster (Chassis)	1562
counters	1563
datapath-debug	1564
decryption-failures	1565
destination-classes	1566
destination-interface	1567
destination-port	1568
fields (for Interface Profiles)	1569
fields (for Routing Engine Profiles)	1570
file (Associating with a Profile)	1571
file (Configuring a Log File)	1572
files	1573
filter-profile	1573
flow (Security Flow)	1574
global-threshold	1576
global-weight	1577
hardware-timestamp	1577
icmp	1578
idp (Security Alarms)	1578
interface-profile	1579
interval	1580
ip-monitoring	1581
ip-monitoring (Services)	1582
maximum-capture-size (Datapath Debug)	1583
mib-profile	1583
mpls (Security Forwarding Options)	1584
next-hop	1584
nonpersistent	1585

object-names	1585
operation	1586
packet-capture	1587
packet-filter	1588
probe	1589
probe-interval	1590
probe-limit	1590
probe-server	1591
probe-type	1592
redundancy-group (Chassis Cluster)	1593
retry-interval (Chassis Cluster)	1594
routing-engine-profile	1595
rpm (Services)	1596
size	1598
source-classes	1598
start-time	1599
target	1599
thresholds	1600
traceoptions (Security Datapath Debug)	1601
transfer-interval	1602
traps	1603
Operational Commands	1603
clear chassis cluster ip-monitoring failure-count	1605
clear chassis cluster ip-monitoring failure-count ip-address	1606
monitor list	1607
monitor start	1608
monitor stop	1610
monitor traffic	1611
mtrace monitor	1621
ping mpls l2circuit	1623
ping mpls l2vpn	1626
ping mpls l3vpn	1629
ping mpls ldp	1632
ping mpls lsp-end-point	1635
ping mpls rsvp	1637
request pppoe connect	1642
request pppoe disconnect	1643
request services ip-monitoring preempt-restore policy	1644
show chassis alarms	1645
show configuration	1647
show chassis cluster ip-monitoring status redundancy-group	1650
show interfaces (SRX Series)	1653
show poe interface (View)	1683
show poe telemetries	1685
show pppoe interfaces	1687
show pppoe statistics	1690
show security alarms	1692
show security datapath-debug capture	1696
show security datapath-debug counter	1697

	show security monitoring fpc fpc-number	1698
	show security monitoring performance session	1701
	show security monitoring performance spu	1702
	show services ip-monitoring status	1703
	show services rpm probe-results (View)	1707
	show system alarms	1711
	traceroute	1712
Chapter 35	System Log Monitoring and Troubleshooting Guide for Security Devices	1717
	Junos OS System Logging	1717
	Introduction to System Logging	1717
	Junos OS System Log Overview	1717
	Junos OS System Logging Facilities and Message Severity Levels	1718
	Junos OS Minimum System Logging Configuration	1719
	Junos OS Default System Log Settings	1720
	Junos OS Platform-Specific Default System Log Messages	1721
	Security Logging	1722
	Configuring System Logging for a Single-Chassis System	1722
	Specifying the Facility and Severity of Messages to Include in the Log	1722
	Directing System Log Messages to a Log File	1723
	Logging Messages in Structured-Data Format	1724
	Directing System Log Messages to a User Terminal	1724
	Directing System Log Messages to the Console	1725
	Including Priority Information in System Log Messages	1725
	System Log Default Facilities for Messages Directed to a Remote Destination	1726
	Including the Year or Millisecond in Timestamps	1727
	Using Regular Expressions to Refine the Set of Logged Messages . .	1728
	Disabling the System Logging of a Facility	1730
	Examples: Configuring System Logging	1730
	Directing System Log Messages to a Remote Destination	1732
	Adding a Text String to System Log Messages	1732
	Adding a String	1733
	Examples: Assigning an Alternative Facility	1733
	Displaying System Log Files	1734
	Displaying a Log File from a Single-Chassis System	1734
	Examples: Displaying a Log File	1734
	Displaying and Interpreting System Log Message Descriptions	1735
	Displaying and Interpreting System Log Message Descriptions	1735
	Interpreting Messages Generated in Structured-Data Format	1737
	The message-source Field on a Single-Chassis System	1742
	Interpreting Messages Generated in Standard Format by Services on a PIC	1742
	Examples: Displaying System Log Message Descriptions	1743

Configuring System Logging for a Security Device	1744
Understanding System Logging for Security Devices	1744
Understanding Binary Format for Security Logs	1746
Configuring Binary Security Log Files	1747
Sending System Log Messages to a File	1748
Setting the System to Send All Log Messages Through eventd	1748
Setting the System to Stream Security Logs Through Revenue Ports	1749
Monitoring System Log Messages with the J-Web Event Viewer	1750
Configuration Statements and Operational Commands	1751
Configuration Statements	1751
allow-duplicates	1753
archive (All System Log Files)	1754
cache (Security Log)	1755
console (System Logging)	1756
destination-override	1757
event-rate	1757
exclude (Security Log)	1758
explicit-priority	1759
facility-override	1759
file (Security Log)	1760
file (System Logging)	1761
files	1762
host (Security Log)	1763
limit (Security Log)	1763
log (Services)	1764
log-prefix (System)	1765
log-rotate-frequency	1765
match	1766
mode (Security Log)	1766
no-remote-trace (System)	1767
pic-services-logging	1767
port	1768
rate-cap	1768
security-log	1769
security-log-percent-full	1770
severity (Security Log)	1770
size	1771
structured-data	1772
syslog (System)	1773
system	1774
time-format	1775
traceoptions (Security Log)	1776
tracing	1778
user (System Logging)	1779
world-readable	1780
Operational Commands	1780
clear log	1781
clear security log	1782

	clear security log file	1784
	monitor list	1785
	monitor start	1786
	monitor stop	1788
	show log	1789
	show security log	1791
	show security log file	1794
Chapter 36	SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices	1797
	Overview	1797
	Introduction to Device Management	1797
	Understanding Device Management Functions in Junos OS	1797
	Understanding the Integrated Local Management Interface	1799
	Network Monitoring Using SNMP	1799
	SNMP MIBs Overview	1800
	Understanding the SNMP Implementation in Junos OS	1800
	SNMP MIBs and Traps Supported by Junos OS	1803
	Standard SNMP MIBs Supported by Junos OS	1804
	Juniper Networks Enterprise-Specific MIBs	1819
	List of SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways Supported Enterprise-Specific MIBs	1826
	List of SRX1400, SRX3400, and SRX3600 Services Gateways Supported Enterprise-Specific MIBs	1830
	List of SRX5400, SRX5600 and SRX5800 Services Gateways Supported Enterprise-Specific MIBs	1836
	Enterprise-Specific MIBs and Supported Devices	1842
	MIB Support Details	1851
	SNMP MIB Objects Supported by Junos OS for the Set Operation	1861
	Juniper Networks Enterprise-Specific SNMP Traps	1868
	Juniper Networks Enterprise-Specific SNMP Version 1 Traps	1869
	Juniper Networks Enterprise-Specific SNMP Version 2 Traps	1876
	Standard SNMP Traps Supported on Devices Running Junos OS	1883
	Standard SNMP Version 1 Traps	1884
	Standard SNMP Version 2 Traps	1887
	Unsupported Standard SNMP Traps	1892
	Loading MIB Files to a Network Management System	1895
	Loading MIB Files to a Network Management System	1895
	Configuring SNMP	1897
	Configuring SNMP on a Device Running Junos OS	1898
	Configuring the System Contact on a Device Running Junos OS	1900
	Configuring the System Location for a Device Running Junos OS	1900
	Configuring the System Description on a Device Running Junos OS	1901
	Configuring the System Name	1901
	Configuring the Commit Delay Timer	1902
	Configuring the SNMP Community String	1902
	Examples: Configuring the SNMP Community String	1903
	Filtering Duplicate SNMP Requests	1904

Configuring the Interfaces on Which SNMP Requests Can Be Accepted	1905
Example: Configuring Secured Access List Checking	1905
Filtering Interface Information Out of SNMP Get and GetNext Output	1905
Configuring MIB Views	1906
Example: Ping Proxy MIB	1907
Configuring SNMP Trap Options and Groups on a Device Running Junos OS	1908
Configuring SNMP Trap Options	1909
Configuring SNMP Trap Groups	1912
Example: Configuring SNMP Trap Groups	1914
Configuring the Trap Notification Filter	1915
Configuring SNMPv3	1916
SNMPv3 Overview	1916
Creating SNMPv3 Users	1917
Example: SNMPv3 Configuration	1918
Example: Creating SNMPv3 Users Configuration	1921
Minimum SNMPv3 Configuration on a Device Running Junos OS	1922
Configuring the SNMPv3 Authentication Type	1923
Configuring the Encryption Type	1925
Defining Access Privileges for an SNMP Group	1926
Configuring the Access Privileges Granted to a Group	1928
Example: Access Privilege Configuration	1931
Assigning Security Model and Security Name to a Group	1932
Example: Security Group Configuration	1933
Example: Configuring the Tag List	1934
Configuring the Local Engine ID	1934
Configuring SNMP Informs	1935
Configuring SNMPv3 Traps on a Device Running Junos OS	1936
Configuring the SNMPv3 Trap Notification	1937
Example: Configuring SNMPv3 Trap Notification	1938
Configuring the Trap Target Address	1939
Defining and Configuring the Trap Target Parameters	1941
Adding a Group of Clients to an SNMP Community	1944
Configuring the SNMPv3 Community	1945
Example: SNMPv3 Community Configuration	1947
Configuring the Inform Notification Type and Target Address	1948
Example: Configuring the Inform Notification Type and Target Address	1949
Configuring the Remote Engine and Remote User	1950
Example: Configuring the Remote Engine ID and Remote Users	1951
Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage	1951
Configuring Routing Instances	1953
Understanding SNMP Support for Routing Instances	1953
Trap Support for Routing Instances	1954

Identifying a Routing Instance	1955
Enabling SNMP Access over Routing Instances	1956
Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community	1956
Example: Configuring Interface Settings for a Routing Instance	1957
Configuring Access Lists for SNMP Access over Routing Instances	1959
Configuring Remote Operations	1959
SNMP Remote Operations Overview	1960
Using the Ping MIB for Remote Monitoring Devices Running Junos OS	1962
Starting a Ping Test	1963
Monitoring a Running Ping Test	1964
Gathering Ping Test Results	1967
Stopping a Ping Test	1968
Interpreting Ping Variables	1968
Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS	1969
Tracing SNMP Activity	1969
Tracing SNMP Activity on a Device Running Junos OS	1969
Example: Tracing SNMP Activity	1973
Configuring Vital MIB Data	1973
Understanding Vital MIB OID Data Collection	1973
Generating Readable Raw OID Data Collections	1974
Generating Raw MIB OID from a Policy	1975
Generating Vital Data of Pre-Defined Group	1976
Generating Vital Data from an Interface	1977
Generating Vital Data from an IPsec VPN	1978
Generating Vital Data from a NAT Rule	1979
Generating Vital Data from an Operating Component	1980
Generating Vital Data from a Screen	1980
SNMP FAQs	1981
Managing Traps and Informs	1981
Remote Monitoring (RMON) with SNMP	1983
RMON Overview	1984
Understanding RMON Alarms	1984
Understanding RMON Events	1985
Configuring RMON Alarms and Events	1986
Understanding RMON Alarms and Events Configuration	1986
Configuring an Alarm Entry and Its Attributes	1987
Configuring an Event Entry and Its Attributes	1991
Example: Configuring an RMON Alarm and Event Entry	1992
Example: Configuring Health Monitoring	1992
Monitoring RMON Alarms and Events	1993
Understanding RMON for Monitoring Service Quality	1993
Understanding Measurement Points, Key Performance Indicators, and Baseline Values	1996
Health Monitoring with SNMP	1998
Configuring Health Monitoring	1998
Configuring Health Monitoring on Devices Running Junos OS	1998

Configuration Statements and Operational Commands	2001
Configuration Statements	2001
Configuration Statements at the [edit snmp] Hierarchy Level	2004
Complete SNMPv3 Configuration Statements	2007
access-list	2010
address	2010
address-mask	2011
agent-address	2011
alarm	2012
authentication-md5	2013
authentication-none	2014
authentication-password	2015
authentication-sha	2016
authorization	2017
categories	2017
client-list	2018
client-list-name	2018
clients	2019
commit-delay	2019
community	2020
community	2021
community-name	2022
contact	2023
description	2023
description	2024
destination-port	2024
engine-id	2025
enterprise-oid	2026
event	2026
falling-event-index	2027
falling-threshold	2028
falling-threshold	2029
falling-threshold-interval	2030
filter-duplicates	2030
filter-interfaces	2031
group (Configuring Group Name)	2032
group (Defining Access Privileges for an SNMPv3 Group)	2033
health-monitor	2033
interface	2034
interval	2034
interval	2035
local-engine	2036
location	2037
logical-system	2038
logical-system-trap-filter	2039
log-vital	2040
message-processing-model	2042
name	2042
nonvolatile	2043

notify	2044
notify-filter (Applying to the Management Target)	2044
notify-filter (Configuring the Profile Name)	2045
notify-view	2045
oid	2046
oid	2046
parameters	2047
port	2047
privacy-3des	2048
privacy-aes128	2049
privacy-des	2050
privacy-none	2050
privacy-password	2051
read-view	2052
remote-engine	2053
request-type	2054
retry-count	2054
rising-event-index	2055
rising-threshold	2055
rising-threshold	2056
rmon	2056
routing-engine (SNMP Resource Level)	2057
routing-engine (SNMP Global Level)	2058
routing-instance	2059
routing-instance	2060
routing-instance-access	2060
sample-type	2061
security-level (Defining Access Privileges)	2062
security-level (Generating SNMP Notifications)	2063
security-model (Access Privileges)	2064
security-model (Group)	2065
security-model (SNMP Notifications)	2065
security-name (Community String)	2066
security-name (Security Group)	2067
security-name (SNMP Notifications)	2068
security-to-group	2069
snmp	2069
source-address	2070
snmp-community	2070
startup-alarm	2071
syslog-subtag	2071
tag	2072
tag-list	2072
target-address	2073
target-parameters	2074
targets	2075
timeout	2075
traceoptions (SNMP)	2076
trap-group	2078

	trap-options	2079
	type	2079
	type	2080
	user	2080
	usm	2081
	v3	2083
	vacm	2085
	variable	2086
	version	2086
	view (Associating a MIB View with a Community)	2087
	view (Configuring a MIB View)	2088
	write-view	2089
	Operational Commands	2089
	show snmp health-monitor	2090
	show snmp health-monitor routing-engine history	2096
	show snmp health-monitor routing-engine status	2100
	show snmp mib (View)	2102
	show system log-vital	2105
Part 7	Standards Reference	
Chapter 37	Overview	2111
	Accessing Standards Documents	2111
	Accessing Standards Documents on the Internet	2111
Chapter 38	Supported Standards	2113
	Chassis and System Standards	2113
	Supported BOOTP and DHCP Standards	2113
	Supported Mobile IP Standards	2114
	Supported Network Management Standards	2115
	Supported RADIUS and TACACS+ Standards for User Authentication	2124
	Supported System Access Standards	2125
	Supported Time Synchronization Standard	2125
	Interface Standards	2126
	Supported ATM Interface Standards	2126
	Supported Ethernet Interface Standards	2126
	Supported Frame Relay Interface Standards	2127
	Supported GRE and IP-IP Interface Standards	2128
	Supported PPP Interface Standards	2128
	Supported SDH and SONET Interface Standards	2129
	Supported Serial Interface Standards	2130
	Supported T3 Interface Standard	2130
	Layer 2 Standards	2131
	Supported Layer 2 Networking Standards	2131
	Supported L2TP Standards	2131
	Supported Layer 2 Circuit Standards	2132
	Supported Layer 2 VPN Standard	2132
	MPLS Applications Standards	2133
	Supported GMPLS Standards	2133
	Supported LDP Standards	2134

Supported MPLS Standards	2135
Supported RSVP Standards	2137
Packet Processing Standards	2138
Supported CoS Standards	2138
Supported Packet Filtering Standards	2139
Supported Policing Standard	2139
Routing Protocol Standards	2140
Supported BGP Standards	2140
Supported ES-IS Standards	2142
Supported ICMP and Neighbor Discovery Standards	2143
Supported IP Multicast Protocol Standards	2143
Supported IPv4, TCP, and UDP Standards	2145
Supported IPv6 Standards	2146
Supported IS-IS Standards	2150
Supported OSPF and OSPFv3 Standards	2151
Supported RIP and RIPvng Standards	2153
Services PIC and DPC Standards	2153
Supported DTCP Standard	2153
Supported Flow Monitoring and Discard Accounting Standards	2154
Supported IPsec and IKE Standards	2154
Supported L2TP Standards	2155
Supported Link Services Standards	2155
Supported NAT and SIP Standards	2156
Supported RPM Standard	2156
Supported Voice Services Standards	2157
VPLS and VPN Standards	2157
Supported Carrier-of-Carriers and Interprovider VPN Standards	2157
Supported Layer 2 VPN Standard	2157
Supported Layer 3 VPN Standards	2158
Supported Multicast VPN Standards	2159
Supported VPLS Standards	2159

Part 8

Index

Index	2163
-----------------	------

List of Figures

Part 1	Junos OS Getting Started Guide for Branch SRX Series	
Chapter 2	Setting Up a Branch SRX Series Services Gateway	5
	Figure 1: SRX210 Deployment Topology	6
	Figure 2: Connecting an SRX210 to the Internet	17
Chapter 3	Configuring Basic SRX Series Features	23
	Figure 3: Topology for Security Policy Configuration	25
	Figure 4: Destination NAT Single Address Translation	31
Part 2	Installation and Upgrade Guide for Security Devices	
Chapter 5	Junos Software and Hardware Overview	123
	Figure 5: Configuration Selection Sequence	129
	Figure 6: SRX240 Device Front Panel	131
	Figure 7: SRX650 Device System Routing Engine	131
	Figure 8: SRX5800 Device Routing Engine	131
Chapter 6	Installing Junos OS Software	133
	Figure 9: Connecting to the Console Port on a Junos OS Device	144
Part 3	CLI User Guide	
Chapter 9	Overview	299
	Figure 10: Monitoring and Configuring Routers	299
	Figure 11: Committing a Configuration	305
	Figure 12: Configuration Statement Hierarchy Example	306
Chapter 12	Using Configuration Statements to Configure a Device	333
	Figure 13: Configuration Mode Hierarchy of Statements	339
Chapter 13	Committing a Junos OS Configuration	371
	Figure 14: Confirm a Configuration	377
Chapter 14	Managing Configurations	389
	Figure 15: Overriding the Current Configuration	401
	Figure 16: Using the replace Option	401
	Figure 17: Using the merge Option	401
	Figure 18: Using a Patch File	402
	Figure 19: Using the set Option	402
Chapter 15	Using Operational Commands to Monitor a Device	413
	Figure 20: Commands That Combine Other Commands	417
	Figure 21: Command Output Options	418

	Figure 22: Restarting a Process	432
Chapter 17	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	447
	Figure 23: Replacement by Object	454
Part 4	J-Web User Guide	
Chapter 23	Overview	577
	Figure 24: J-Web Layout	587
	Figure 25: Top Pane Elements	587
	Figure 26: Main Pane Elements	588
	Figure 27: Side Pane Elements	589
	Figure 28: CoS Help Page	591
	Figure 29: View Configuration Text Page	596
	Figure 30: Edit Configuration Text Page	597
	Figure 31: Starting the CLI Terminal	599
	Figure 32: J-Web CLI Terminal	601
Chapter 24	Configuring a Device Using J-Web	603
	Figure 33: Edit Management Access Page	606
	Figure 34: J-Web Set Up Initial Configuration Page	610
	Figure 35: Edit Configuration Page	613
	Figure 36: Accounting Options Configuration Editor Page	617
Chapter 25	Administering a Device Using J-Web	619
	Figure 37: Configuration Database and History Page	620
	Figure 38: Database Information Page	622
	Figure 39: J-Web Configuration File Comparison Results	624
	Figure 40: J-Web Upload Configuration File Page	625
	Figure 41: Manage Snapshots Page	627
	Figure 42: View Alarms Page	630
	Figure 43: View Events page	631
	Figure 44: J-Web View Events Page	636
	Figure 45: Sample RPM Graphs	640
	Figure 46: Port Monitoring Page	646
	Figure 47: Details of Interface ge-0/0/0 Page	647
	Figure 48: Monitoring Route Information Page with Complete Information	648
	Figure 49: Monitoring Route Information Page with Selective Information	648
Chapter 26	Troubleshooting	651
	Figure 50: View Events Page Displaying Error	652
	Figure 51: Verifying System Log Messages Configuration	653
	Figure 52: Ping Host Troubleshoot Page	657
	Figure 53: Successful Ping Host Results Page	658
	Figure 54: Unsuccessful Ping Host Results Page	659
Part 5	Administration Guide for Security Devices	
Chapter 29	Configuring DNS	905
	Figure 55: DNS Proxy with Split DNS	911
	Figure 56: Dynamic DNS	913

Part 6	Monitoring and Troubleshooting Library for Security Devices
Chapter 34	Network Monitoring and Troubleshooting Guide for Security Devices . . 1283
	Figure 57: Sample RPM Graphs 1341
	Figure 58: IP Monitoring on a High-End SRX Series Device Topology Example . . 1350
	Figure 59: PPP and MLPPP Headers 1539
Chapter 36	SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices 1797
	Figure 60: Inform Request and Response 1936
	Figure 61: SNMP Data for Routing Instances 1954
	Figure 62: Setting Thresholds 1993
	Figure 63: Network Entry Points 1997

List of Tables

	About the Documentation	liii
	Table 1: Notice Icons	lv
	Table 2: Text and Syntax Conventions	lv
Part 1	Junos OS Getting Started Guide for Branch SRX Series	
Chapter 2	Setting Up a Branch SRX Series Services Gateway	5
	Table 3: Default Interfaces Settings	7
	Table 4: Default Security Policy Settings	7
	Table 5: Default NAT Settings	8
	Table 6: Settings Used to Configure the SRX210	14
Chapter 3	Configuring Basic SRX Series Features	23
	Table 7: Factory-Default Settings for Security Policies for Branch SRX Series Devices	24
	Table 8: Address Books Configuration	26
	Table 9: Security Policy Configuration	26
	Table 10: Destination NAT Mapping	31
	Table 11: Default UTM Profiles on Branch SRX Series	37
Chapter 4	Configuration Statements and Operational Commands	57
	Table 12: show security flow session Output Fields	92
	Table 13: show security idp active-policy Output Fields	97
	Table 14: show security idp status Output Fields	98
	Table 15: show security nat destination summary Output Fields	100
	Table 16: show security policies Output Fields	103
	Table 17: show security zones Output Fields	112
	Table 18: show system license Output Fields	115
	Table 19: show system services dhcp client Output Fields	118
Part 2	Installation and Upgrade Guide for Security Devices	
Chapter 5	Junos Software and Hardware Overview	123
	Table 20: Storage Media Names	132
Chapter 6	Installing Junos OS Software	133
	Table 21: show system download Output Fields	136
	Table 22: Environment Variables Settings	149
	Table 23: Interfaces and Protocols for IP Address Acquisition During Autoinstallation	152
	Table 24: Storage Media on SRX Series Devices	157
	Table 25: Secondary Storage Devices for SRX Series Devices	171

	Table 26: Install Package Summary	176
	Table 27: CLI Commands for Manual BIOS Upgrade	177
	Table 28: Autorecovery Alarms	185
Chapter 7	Installing and Managing Software Licenses	195
	Table 29: Summary of License Management Fields	197
	Table 30: Junos OS Feature Licenses	198
	Table 31: Junos OS Feature License Model Number for SRX Series Devices	200
Chapter 8	Configuration Statements and Operational Commands	217
	Table 32: show system auto-snapshot Output Fields	281
	Table 33: show system autorecovery state Output Fields	283
	Table 34: show system download Output Fields	285
	Table 35: show system license Output Fields	287
	Table 36: show system storage Output Fields	291
Part 3	CLI User Guide	
Chapter 9	Overview	299
	Table 37: Concurrent J-Web Sessions on SRX Series Devices	302
	Table 38: Concurrent CLI Sessions on SRX Series Devices	303
	Table 39: CLI Configuration Mode Navigation Commands	306
Chapter 12	Using Configuration Statements to Configure a Device	333
	Table 40: Summary of Configuration Mode Commands	336
	Table 41: Configuration Mode Top-Level Statements	338
	Table 42: Forms of the configure Command	343
Chapter 14	Managing Configurations	389
	Table 43: CLI Configuration Input Types	397
Chapter 15	Using Operational Commands to Monitor a Device	413
	Table 44: Commonly Used Operational Mode Commands	415
	Table 45: Directories on the Router	424
	Table 46: show system process extensive Command Output Fields	431
Chapter 16	Filtering Command Output	437
	Table 47: Common Regular Expression Operators in Operational Mode Commands	438
Chapter 17	Using Shortcuts, Wildcards, and Regular Expressions in the CLI	447
	Table 48: CLI Keyboard Sequences	448
	Table 49: Wildcard Characters for Specifying Interface Names	449
	Table 50: Common Regular Expressions to Use with the replace Command	450
	Table 51: Replacement Examples	451
Chapter 21	Junos OS CLI Environment Commands	521
	Table 52: show cli Output Fields	532
Chapter 22	Junos OS CLI Operational Mode Commands	537
	Table 53: show system commit Output Fields	572

Part 4	J-Web User Guide	
Chapter 23	Overview	577
	Table 54: Concurrent J-Web Sessions on SRX Series Devices	580
	Table 55: Concurrent CLI Sessions on SRX Series Devices	581
	Table 56: Concurrent Web Sessions on SRX Series Devices	582
	Table 57: Key J-Web Edit Configuration Buttons	590
	Table 58: Junos OS Configuration Terms	592
	Table 59: J-Web Configuration Editor Tasks Summary	593
Chapter 24	Configuring a Device Using J-Web	603
	Table 60: Secure Access Configuration Summary	607
	Table 61: Initial Configuration Set Up Summary	610
	Table 62: J-Web Configuration Tasks Summary	612
	Table 63: J-Web Edit Configuration Links	614
	Table 64: J-Web Edit Configuration Icons	614
	Table 65: J-Web Edit Configuration Buttons	615
Chapter 25	Administering a Device Using J-Web	619
	Table 66: J-Web Configuration History Summary	620
	Table 67: J-Web Configuration Database Information Summary	622
	Table 68: Manage Files Tasks Summary	625
	Table 69: Severity Levels	632
	Table 70: Summary of Event Filters	633
	Table 71: Common Regular Expression Operators and the Terms They Match	634
	Table 72: Class of Service Information and the Corresponding CLI show Commands	637
	Table 73: Interfaces Information and the Corresponding CLI show Commands	638
	Table 74: MPLS Information and the Corresponding CLI show Commands	638
	Table 75: RPM Information and the Corresponding CLI show Command	639
	Table 76: Routing Information and the Corresponding CLI show Commands	640
	Table 77: Firewall Information and the Corresponding CLI show Commands	642
	Table 78: IPsec Information and the Corresponding CLI show Commands	642
	Table 79: NAT Information and the Corresponding CLI show Command	643
	Table 80: Service Sets Information and the Corresponding CLI show Commands	643
	Table 81: DHCP Information and the Corresponding CLI show Commands	643
	Table 82: System Information and the Corresponding CLI show Commands	644
	Table 83: Chassis Information and the Corresponding CLI show Commands	644
	Table 84: Process Details Information and the Corresponding CLI show Commands	645
	Table 85: FEB Redundancy Information and the Corresponding CLI show Command	645
Chapter 26	Troubleshooting	651
	Table 86: Ping MPLS Tasks Summary and the Corresponding CLI show Commands	655
	Table 87: J-Web Ping Host Results and Output Summary	658

Part 5	Administration Guide for Security Devices	
Chapter 27	User Access and Authentication	663
	Table 88: Predefined Login Classes	663
	Table 89: Permission Bits for Login Classes	664
	Table 90: Login Class Permission Flags	669
Chapter 28	Configuring Remote Access to an SRX Series Appliances	865
	Table 91: Default Modem Initialization Commands	874
	Table 92: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity	876
	Table 93: Incoming Map Options	877
	Table 94: CLI telnet Command Options	899
	Table 95: CLI ssh Command Options	900
Chapter 30	Configuring DHCP Access Service for IP Address Management	917
	Table 96: Sample DHCP Server Configuration Settings	924
	Table 97: DHCPv6 Attributes	957
Chapter 31	Managing System Files	977
	Table 98: request system set-encryption-key Commands	978
Chapter 32	Working with Junos OS Licenses	989
	Table 99: Summary of License Management Fields	990
	Table 100: Junos OS Feature Licenses	991
	Table 101: Junos OS Feature License Model Number for SRX Series Devices	992
Chapter 33	Configuration Statements and Operational Commands	1009
	Table 102: Sample show Commands Called by the request information support command on an MX Series Router	1209
	Table 103: show chassis routing-engine Output Fields	1230
	Table 104: show dhcp client binding Output Fields	1234
	Table 105: show dhcp client statistics	1237
	Table 106: show dhcp relay binding Output Fields	1239
	Table 107: show dhcp relay statistics	1241
	Table 108: show dhcp server binding Output Fields	1243
	Table 109: show dhcp server statistics	1245
	Table 110: show dhcpv6 client binding Output Fields	1247
	Table 111: show dhcpv6 client statistics Output Fields	1249
	Table 112: show dhc6p server binding Output Fields	1251
	Table 113: show dhcpv6 server statistics Output Fields	1256
	Table 114: show firewall Output Fields	1258
	Table 115: show system autorecovery state Output Fields	1260
	Table 116: show system directory-usage Output Fields	1262
	Table 117: show system download Output Fields	1264
	Table 118: show system license Output Fields	1266
	Table 119: show system login lockout	1269
	Table 120: show system services dhcp client Output Fields	1270
	Table 121: show system services dhcp relay-statistics Output Fields	1273
	Table 122: show system storage Output Fields	1276

Part 6

Chapter 34

Monitoring and Troubleshooting Library for Security Devices

Network Monitoring and Troubleshooting Guide for Security Devices . . 1283

Table 123: J-Web Interface Troubleshoot Options	1285
Table 124: CLI Diagnostic Command Summary	1286
Table 125: Types of Accounting Profiles	1287
Table 126: Interface Alarm Conditions	1312
Table 127: System Alarm Conditions and Corrective Actions	1315
Table 128: Alarms Monitoring Page	1320
Table 129: RPM Statistics	1323
Table 130: RPM Configuration Summary	1337
Table 131: Summary of Key RPM Output Fields	1341
Table 132: Test Parameters and Default Values	1345
Table 133: Threshold Supported and Description	1346
Table 134: CLI mtrace from-source Command Options	1358
Table 135: CLI mtrace from-source Command Output Summary	1359
Table 136: CLI traceroute monitor Command Options	1360
Table 137: CLI traceroute monitor Command Output Summary	1361
Table 138: Summary of Key H.323 Counters Output Fields	1363
Table 139: Summary of Key MGCP Calls Output Fields	1364
Table 140: Summary of Key MGCP Counters Output Fields	1365
Table 141: Summary of Key MGCP Endpoints Output Fields	1366
Table 142: Summary of Key SCCP Calls Output Fields	1367
Table 143: Summary of Key SCCP Counters Output Fields	1368
Table 144: Summary of Key SIP Calls Output Fields	1370
Table 145: Summary of Key SIP Counters Output Fields	1370
Table 146: Summary of Key SIP Rate Output Fields	1372
Table 147: Summary of Key SIP Transactions Output Fields	1373
Table 148: ALG H.323 Monitoring Page	1374
Table 149: Voice ALG MGCP Monitoring Page	1376
Table 150: Voice ALG SCCP Monitoring Page	1378
Table 151: Voice ALG SIP Monitoring Page	1381
Table 152: Voice ALG Summary Monitoring Page	1386
Table 153: Summary of Key CoS Interfaces Output Fields	1387
Table 154: Summary of Key CoS Classifier Output Fields	1388
Table 155: Summary of Key CoS Value Alias Output Fields	1389
Table 156: Summary of Key CoS RED Drop Profile Output Fields	1390
Table 157: Summary of Key CoS Forwarding Class Output Fields	1391
Table 158: Summary of Key CoS Rewrite Rules Output Fields	1391
Table 159: Summary of Key CoS Scheduler Maps Output Fields	1392
Table 160: Summary of Key CoS Classifier Output Fields	1394
Table 161: CLI monitor interface Output Control Keys	1395
Table 162: CLI monitor interface traffic Output Control Keys	1395
Table 163: Address Pools Monitoring Page	1397
Table 164: Summary of Ethernet Switching Output Fields	1398
Table 165: GVRP Monitoring Page	1399
Table 166: Summary of Key MPLS Interface Information Output Fields	1402
Table 167: Summary of Key MPLS LSP Information Output Fields	1402
Table 168: Summary of Key MPLS LSP Statistics Output Fields	1403

Table 169: Summary of Key RSVP Session Information Output Fields	1404
Table 170: Summary of Key RSVP Interfaces Information Output Fields	1405
Table 171: Summary of Key PPPoE Output Fields	1407
Table 172: Spanning Tree Monitoring Page	1410
Table 173: Source NAT Monitoring Page	1412
Table 174: Summary of Key Destination NAT Output Fields	1418
Table 175: Summary of Key Static NAT Output Fields	1420
Table 176: Summary of Key Incoming Table Output Fields	1421
Table 177: Summary of Key Interface NAT Output Fields	1422
Table 178: Filtering Route Messages	1424
Table 179: Summary of Key Routing Information Output Fields	1425
Table 180: Summary of Key RIP Routing Output Fields	1426
Table 181: Summary of Key OSPF Routing Output Fields	1427
Table 182: Summary of Key BGP Routing Output Fields	1429
Table 183: View Policy Log Fields	1430
Table 184: Policy Events Detail Fields	1432
Table 185: Security Policies Monitoring Output Fields	1433
Table 186: Check Policies Output	1436
Table 187: Summary of Key Screen Counters Output Fields	1438
Table 188: Summary of IDP Status Output Fields	1441
Table 189: Summary of Key Flow Gate Output Fields	1442
Table 190: Summary of Key Firewall Authentication Table Output Fields	1443
Table 191: Summary of Key Firewall Authentication History Output Fields	1444
Table 192: Summary of Dot1X Output Fields	1446
Table 193: Summary of Key DHCP Client Binding Output Fields	1447
Table 194: Events Monitoring Page	1448
Table 195: Statistics Tab Output in the Threats Report	1460
Table 196: Activities Tab Output in the Threats Report	1462
Table 197: Traffic Report Output	1464
Table 198: Summary of Key IKE SA Information Output Fields	1467
Table 199: IPsec VPN—Phase I Monitoring Page	1470
Table 200: IPsec VPN—Phase II Monitoring Page	1471
Table 201: Summary of Key IPsec VPN Information Output Fields	1473
Table 202: CLI mtrace monitor Command Output Summary	1486
Table 203: Traceroute Field Summary	1487
Table 204: J-Web Traceroute Results and Output Summary	1488
Table 205: CLI traceroute Command Options	1490
Table 206: Options for Checking MPLS Connections	1492
Table 207: CLI ping Command Options	1495
Table 208: J-Web Ping Host Field Summary	1497
Table 209: Ping Host Results and Output	1498
Table 210: J-Web Ping MPLS Field Summary	1500
Table 211: J-Web Ping MPLS Results and Output Summary	1502
Table 212: CLI ping mpls l2circuit Command Options	1504
Table 213: CLI ping mpls l2vpn Command Options	1505
Table 214: CLI ping mpls l3vpn Command Options	1506
Table 215: CLI ping mpls ldp and ping mpls lsp-end-point Command Options	1507
Table 216: CLI monitor traffic Command Options	1523
Table 217: CLI monitor traffic Match Conditions	1525

	Table 218: CLI monitor traffic Logical Operators	1526
	Table 219: CLI monitor traffic Arithmetic, Binary, and Relational Operators	1527
	Table 220: Packet Capture Field Summary	1528
	Table 221: J-Web Packet Capture Results and Output Summary	1531
	Table 222: CoS Components Applied on Multilink Bundles and Constituent Links	1535
	Table 223: PPP and MLPPP Encapsulation Overhead	1539
	Table 224: Number of Packets Transmitted on a Queue	1542
	Table 225: monitor list Output Fields	1607
	Table 226: monitor start Output Fields	1608
	Table 227: Match Conditions for the monitor traffic Command	1613
	Table 228: Logical Operators for the monitor traffic Command	1614
	Table 229: Arithmetic and Relational Operators for the monitor traffic Command	1616
	Table 230: mtrace monitor Output Fields	1621
	Table 231: show chassis alarms Output Fields	1645
	Table 232: show chassis cluster ip-monitoring status Output Fields	1650
	Table 233: show chassis cluster ip-monitoring status redundancy group Reason Fields	1651
	Table 234: show interfaces Output Fields	1655
	Table 235: show poe interface Output Fields	1683
	Table 236: show poe telemetries interface Output Fields	1685
	Table 237: show pppoe interfaces Output Fields	1687
	Table 238: show pppoe statistics Output Fields	1690
	Table 239: show security alarms	1693
	Table 240: show security monitoring fpc fpc-number Output Fields	1698
	Table 241: show services ip-monitoring status Output Fields	1703
	Table 242: show services rpm probe-results Output Fields	1707
	Table 243: traceroute Output Fields	1714
Chapter 35	System Log Monitoring and Troubleshooting Guide for Security Devices	1717
	Table 244: Junos OS System Logging Facilities	1718
	Table 245: System Log Message Severity Levels	1719
	Table 246: Minimum Configuration Statements for System Logging	1719
	Table 247: Default System Logging Settings	1720
	Table 248: Default Facilities for Messages Directed to a Remote Destination	1727
	Table 249: Regular Expression Operators for the match Statement	1729
	Table 250: Fields in System Log Message Descriptions	1736
	Table 251: Fields in Structured-Data Messages	1738
	Table 252: Facility and Severity Codes in the priority-code Field	1739
	Table 253: Platform Identifiers in the platform Field	1741
	Table 254: Fields in Messages Generated by a PIC	1742
	Table 255: monitor list Output Fields	1785
	Table 256: monitor start Output Fields	1786
	Table 257: show security log Output Fields	1792
	Table 258: show security log file Output Fields	1794
Chapter 36	SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices	1797

Table 259: Device Management Features in Junos OS	1798
Table 260: Standard MIBs Supported on Devices Running Junos OS	1804
Table 261: Enterprise-Specific MIBs and Supported Devices	1842
Table 262: MIB Support for Routing Instances (Juniper Networks MIBs)	1851
Table 263: Class 1 MIB Objects (Standard and Juniper MIBs)	1855
Table 264: Class 2 MIB Objects (Standard and Juniper MIBs)	1859
Table 265: Class 3 MIB Objects (Standard and Juniper MIBs)	1860
Table 266: Class 4 MIB Objects (Standard and Juniper MIBs)	1861
Table 267: SNMP MIB Objects	1861
Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps	1869
Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps	1876
Table 270: Standard Supported SNMP Version 1 Traps	1884
Table 271: Standard Supported SNMP Version 2 Traps	1888
Table 272: Unsupported Standard SNMP Traps	1893
Table 273: Results in pingProbeHistoryTable: After the First Ping Test	1967
Table 274: Results in pingProbeHistoryTable: After the First Probe of the Second Test	1967
Table 275: Results in pingProbeHistoryTable: After the Second Ping Test	1968
Table 276: SNMP Tracing Flags	1972
Table 277: RMON Event Table	1995
Table 278: RMON Alarm Table	1995
Table 279: jnxRmon Alarm Extensions	1996
Table 280: Monitored Object Instances	1999
Table 281: show snmp health-monitor Output Fields	2090
Table 282: show snmp health-monitor routing engine history Output Fields	2096
Table 283: show snmp health-monitor routing engine status Output Fields	2100
Table 284: show snmp mib Output Fields	2103
Table 285: show system log-vital Output fields	2105

About the Documentation

- Documentation and Release Notes on page liii
- Supported Platforms on page liii
- Using the Examples in This Manual on page liii
- Documentation Conventions on page lv
- Documentation Feedback on page lvii
- Requesting Technical Support on page lvii

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>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- [SRX Series](#)

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 on page lv](#) 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 on page lv](#) 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

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<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.

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

Convention	Description	Examples
> (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>.

PART 1

Junos OS Getting Started Guide for Branch SRX Series

- [Overview on page 3](#)
- [Setting Up a Branch SRX Series Services Gateway on page 5](#)
- [Configuring Basic SRX Series Features on page 23](#)
- [Configuration Statements and Operational Commands on page 57](#)

CHAPTER 1

Overview

- [Introduction to SRX Series Devices on page 3](#)

Introduction to SRX Series Devices

- [SRX Series Overview on page 3](#)

SRX Series Overview

Juniper Networks SRX Series Services Gateways provide high-performance security, routing, and network solutions for enterprise and service providers. The SRX Series pack high port density, advanced security, and flexible connectivity into a single, easily managed platform that supports fast, secure, and highly available data center and branch operations.

The SRX Series are based on Junos OS, a full-featured networking operating system that is optimized to provide maximum performance and efficient network security.

The SRX Series range from lower-end branch devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The branch SRX Series include the SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Understanding Methods to Manage the Branch SRX Series on page 13](#)

CHAPTER 2

Setting Up a Branch SRX Series Services Gateway

- Understanding Factory Default Configuration Settings on page 5
- Configuring an SRX Series Device for the First Time on page 13
- Resetting the SRX Series Device on page 21

Understanding Factory Default Configuration Settings

- Understanding Factory Default Configuration Settings of an SRX210 on page 5
- SRX210 Factory Default Settings—A Sample on page 8

Understanding Factory Default Configuration Settings of an SRX210

This topic includes the following sections:

- Default Configuration Topology on page 5
- Default Port Settings on page 6
- Default Settings for Interfaces, Zones, Policy, and NAT on page 7
- Default System Services on page 8
- Autoinstallation on page 8

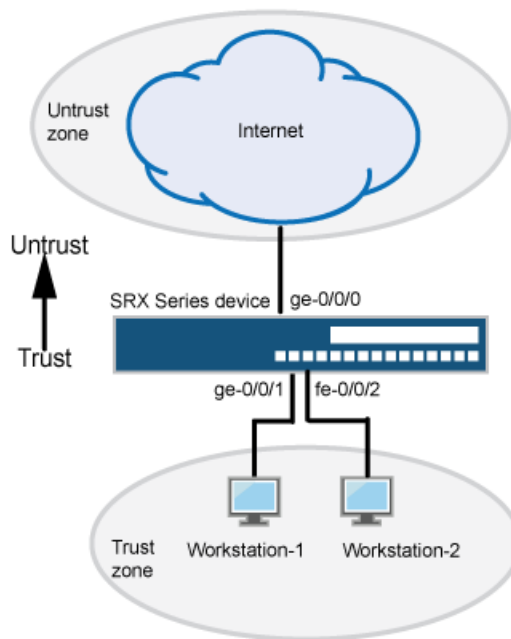
Default Configuration Topology

Figure 1 on page 6 provides a topology of a simple network consisting of the SRX210.



NOTE: This document describes how to set up a basic configuration for a branch SRX Series Services Gateway for the first time. This document uses an SRX210 Services Gateway as an example. For additional details, see the SRX210 Services Gateway Hardware Guide at [SRX210 Services Gateway Hardware](#).

Figure 1: SRX210 Deployment Topology



In a typical deployment scenario of the SRX210, the following configurations are used:

- The SRX Series interface ge-0/0/0 is connected to a typical Internet service provider (ISP) cable or DSL modem.
- The protected network is connected to interface ge-0/0/1, fe-0/0/2 to fe-0/0/7 in the trust zone.
- The IP address of interface ge-0/0/0 is assigned from ISP either statically or by DHCP.
- The interfaces ge-0/0/1, fe-0/0/2 to fe-0/0/7 are a part of the default VLAN (**vlan-trust**). The protected hosts can be connected to any one of the ports that are part of the default VLAN.
- The DHCP server is running on vlan.0 and assigns IP addresses to other interfaces for the local LAN.
- The default security policy allows traffic from the trust zone to the untrust zone and denies traffic from the untrust to trust zone.
- System services such as SSH, Telnet, FTP, HTTP, HTTPS, and xnm-clear-text are enabled by default.

Default Port Settings

When an SRX210 is powered on for the first time, it boots using the factory default configuration.

The SRX210 has the following factory default port settings:

- WAN interface—The Ethernet interface labeled **0/0** on the services gateway chassis (called as ge-0/0/0 in J-Web and the CLI) is in Layer 3 (routing) mode.

This WAN interface is used to connect your services gateway to your ISP. By default, the WAN port is a Dynamic Host Control Protocol (DHCP) client and configured to receive an IP address through DHCP.

- LAN interfaces—Ethernet interfaces labeled **0/1** through **0/7** (called as ge-0/0/1, fe-0/0/2 to fe-0/0/7) are in Layer 2 mode (Ethernet switching mode) and assigned to a VLAN (**vlan-trust**).

A VLAN interface (Layer 3 interface) is created to route traffic from the interfaces in the LAN (ge-0/0/1, fe-0/0/2 to fe-0/0/7) to WAN (ge-0/0/0) interface and vice versa. All traffic between the ports within the VLAN is locally switched. The trust zone VLAN interface (vlan.0) has a default static IP of 192.168.1.1/24, and assigns IP addresses in the 192.168.1.2 to 192.168.1.254 range to any device plugged into the trust interfaces.

Default Settings for Interfaces, Zones, Policy, and NAT

Table 3 on page 7 provides the default configuration of the interfaces on an SRX210.

Table 3: Default Interfaces Settings

Interface	Security Zones	DHCP State	IP Address
ge-0/0/0	Untrust	Client	Dynamically assigned
vlan.0	Trust	Server	192.168.1.1/24



NOTE: Because Ethernet interfaces (ge-0/0/1, fe-0/0/2 to fe-0/0/7) are assigned to the trust zone (vlan-trust), any traffic originating from these interfaces is treated as trust.

Table 4 on page 7 provides the default security policies to block traffic coming from the untrust zone to devices in the trust zone.

Table 4: Default Security Policy Settings

Source Zone	Destination Zone	Policy Action
Trust	Untrust	Permit
Untrust	Trust	Deny



NOTE: In default configuration, all LAN interfaces are in Layer 2 mode and they communicate with each other without need of any policy.

[Table 5 on page 8](#) provides outbound Internet access using source NAT with port address translation, permitting traffic from the trust zone to the untrust zone.

Table 5: Default NAT Settings

Source Zone	Destination Zone	Policy Action
Trust	Untrust	Source NAT to the untrust zone interface

See [“SRX210 Factory Default Settings—A Sample” on page 8](#) to view the factory default configuration of the device.

Default System Services

The following system services are enabled by default on a branch SRX Series:

- DHCP
- FTP
- HTTP
- HTTPS
- SSH
- Telnet
- xnm-clear-text

Autoinstallation

Autoinstallation provides automatic configuration for a new device that you connect to the network. Autoinstallation is active by default and is deactivated when you commit the device for the first time.

You can use the **delete system autoinstallation** command to delete autoinstallation.

For more details on Autoinstallation, see *Installation and Upgrade Guide for Security Devices*.

Related Documentation

- [SRX Series Overview on page 3](#)
- [SRX210 Factory Default Settings—A Sample on page 8](#)
- [Understanding Methods to Manage the Branch SRX Series on page 13](#)

SRX210 Factory Default Settings—A Sample

The following sample output shows the factory default configuration of an SRX210:

```
[edit]
user@srx210-host# show system
system {
  autoinstallation {
    delete-upon-commit; ## Deletes [system autoinstallation] upon change/commit
```

```
traceoptions {
  level verbose;
  flag {
    all;
  }
}
interfaces {
  ge-0/0/0 {
    bootp;
  }
}
name-server {
  208.67.222.222;
  208.67.220.220;
}
services {
  ssh;
  telnet;
  xnm-clear-text;
  web-management {
    http {
      interface vlan.0;
    }
    https {
      system-generated-certificate;
      interface vlan.0;
    }
  }
  dhcp {
    router {
      192.168.1.1;
    }
    pool 192.168.1.0/24 {
      address-range low 192.168.1.2 high 192.168.1.254;
    }
    propagate-settings ge-0/0/0.0;
  }
}
syslog {
  archive size 100k files 3;
  user * {
    any emergency;
  }
  file messages {
    any critical;
    authorization info;
  }
  file interactive-commands {
    interactive-commands error;
  }
}
max-configurations-on-flash 5;
max-configuration-rollback 5;
license {
  autoupdate {
```

```
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
## Warning: missing mandatory statement(s): 'root-authentication'
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/2 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/3 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/4 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/5 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
        }
    }
    fe-0/0/6 {
        unit 0 {
```



```

        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/7 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members vlan-trust;
            }
        }
    }
}
vlan {
    unit 0 {
        family inet {
            address 192.168.1.1/24;
        }
    }
}
}
protocols {
    stp;
}
security {
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
            }
            land;
        }
    }
}
nat {
    source {
        rule-set trust-to-untrust {
            from zone trust;
            to zone untrust;
            rule source-nat-rule {
                match {

```

Copyright © 2016, Juniper Networks, Inc.

```

        vlan-id 3;
        l3-interface vlan.0;
    }
}

```

**Related
Documentation**

- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

Configuring an SRX Series Device for the First Time

- [Understanding Methods to Manage the Branch SRX Series on page 13](#)
- [Mandatory Settings to Configure the Branch SRX Series on page 14](#)
- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)
- [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)
- [Configuring Internet Access for the Branch SRX Series on page 17](#)
- [Configuring a Network Time Protocol Server for the Branch SRX Series on page 18](#)
- [Validating the Branch SRX Series Configuration on page 19](#)
- [Verifying the Branch SRX Series Configuration on page 20](#)

Understanding Methods to Manage the Branch SRX Series

You can use a PC or laptop to configure and monitor your SRX Series. The branch SRX Series have a factory default configuration that enables you to connect to devices through any of the following methods right out of the box:

- **Connecting through the console port**—Use an Ethernet cable with an RJ-45 to DB-9 serial port adapter to connect the console port on the SRX Series to the serial port on the PC or laptop. This connection method does not require any prior configuration on the SRX Series.
- **Connecting through the J-Web interface**—J-Web is a powerful Web-based interface that allows you to manage the SRX Series through a graphical interface on a Web browser. Use an RJ-45 Ethernet cable to connect the PC or laptop to one of the Ethernet ports labeled **0/1** through **0/7** on the front panel of your services gateway.

To access the J-Web setup wizard, open a Web browser on the PC or laptop and enter the IP address 192.168.1.1 in the address field. Log in using the default user name “root”, with a blank password field. No prior configuration is required.

- **Connecting through SSH and Telnet**—Use an RJ-45 Ethernet cable to connect the PC or laptop to one of the Ethernet ports labeled **0/1** through **0/7** on the front panel of your services gateway.



NOTE: To access the device through SSH and Telnet, you need to set up a root password. For more details, see *Connecting Your Branch SRX Series for the First Time*.

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)

Mandatory Settings to Configure the Branch SRX Series

[Table 6 on page 14](#) provides the details on configuration settings that you need to enter when configuring the device for the first time.

Table 6: Settings Used to Configure the SRX210

Settings	Details
Administrator Username	Record the login name of the services gateway administrator. Default is root, which you must change during your first J-Web session.
Administrator Password	Record the password for this administrator account.
Hostname	Record the name of your SRX210 to identify itself on your network.
Network Time Protocol (NTP) Server	Network security often depends on knowing the exact time, when a specific event occurs. If you do not have access to a private NTP server, you can enter the name or IP address of a public NTP server. For information about public time servers, see http://tf.nist.gov/tf-cgi/servers.cgi .
Time Zone	Record the time zone to be used by your services gateway.
IP address assignment	<p>Your Internet Service Provider might use the Dynamic Host Configuration Protocol (DHCP) to assign an IP address and routing information to your services gateway.</p> <p>NOTE: The DHCP client configuration is by default enabled on port 0/0 (ge-0/0/0).</p> <p>NOTE: If your ISP does not support DHCP, you should ask your ISP what settings (IP address, default gateway, DNS server) to use to configure the WAN interface on your services gateway.</p>

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)

Connecting the Branch SRX Series Through the Console Port for the First Time

The following procedure describes the steps required to connect a branch SRX Series through the console port for the first time.

To connect the device:

1. Connect your computer or laptop to the RJ-45 console port on the SRX Series .
2. Start the terminal emulation program on the computer or laptop, select the COM port, and configure the following port settings:
 - Bits per second—9600
 - Data bits—8
 - Parity—none
 - Stop bits—1
 - Flow control—none
3. Click Open or Connect (the term varies in different applications).
4. Press the **POWER** button on the device, and wait till the Power LED turns green.
5. Log in to the device as root and leave the password field blank. When you boot the device with the factory default configuration, you do not need a password.
6. Enter the UNIX shell after you are authenticated through the CLI:

```
Amnesiac (ttyu0)
login: root
Password:
--- JUNOS 12.1X44-D10.4 built 2013-01-08 05:15:31 UTC
```

7. At the % prompt, type **cli** to start the CLI and press Enter. The prompt changes to an angle bracket (>) when you enter CLI operational mode.

```
root@% cli
root>
```

8. At the (>) prompt, type **configure** and press Enter. The prompt changes from > to # when you enter configuration mode.

```
root> configure
Entering configuration mode
[edit]
root#
```

9. Create a password for the root user to manage the SRX Series.

```
set system root authentication plain-text-password
```

Enter a password at the New password prompt, then confirm by entering the same password at the Retype New password prompt.

New password:
Retype New password:

At the CLI prompt, type **commit** to activate the configuration.

Now, proceed with configuring system identification settings, users and classes. See “Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network” on page 16.



NOTE: If you are unable to log in with the username **root** and no password, it could be because the device has a different configuration than the factory settings. If you do not know the password of the **root** account, or any another account with super-user privileges, then a password reset is required. The process to do a password recovery can be found here: <http://kb.juniper.net/KB12167>.

**Related
Documentation**

- [Understanding Methods to Manage the Branch SRX Series on page 13](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network

The following procedure describes the steps required to configure a hostname for a branch SRX Series Services Gateway to identify it in your network topology maps and to remind you which device you are logged into.

1. In configuration mode configure a hostname for the branch SRX Series Services Gateway.

```
[edit]  
root# set system host-name SRX210
```

2. At the CLI prompt, type the **commit** command to activate the configuration.

```
[edit]  
root# commit  
  
root# commit  
commit complete  
  
[edit]  
root@SRX210#
```



NOTE: If after following this procedure you still require further guidance on configuring a branch SRX Series Services Gateway, see *Quick Start Guide* of your device.

**Related
Documentation**

- [Mandatory Settings to Configure the Branch SRX Series on page 14](#)

- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)

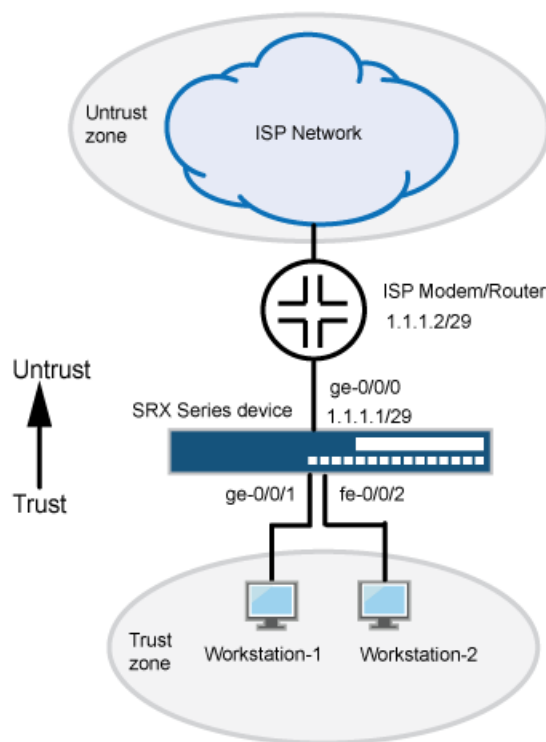
Configuring Internet Access for the Branch SRX Series

Connect the port on the SRX210 that you want to use for Internet access (typically the port labeled **0/0**) to the cable modem or to the connection device provided by your Internet service provider (ISP). You can enable Internet access in the following ways:

- Assign an IP address and gateway through DHCP—If your ISP supports DHCP, your services gateway acquires an IP address and other settings (domain name servers, default routes) from your ISP.
- Assign IP address manually—If your ISP does not provide IP address information through DHCP, you can configure the gateway WAN port with a static IP address and a default route.

[Figure 2 on page 17](#) shows connecting an SRX210 to the Internet.

Figure 2: Connecting an SRX210 to the Internet



To assign an IP address and gateway through DHCP:

1. Configure interface **ge-0/0/0** to obtain an IP address and default gateway from a DHCP server:

[edit]

```
root@host# set interfaces ge-0/0/0 unit 0 family inet dhcp
```

To assign an IP address and gateway manually:

1. Configure a static default route pointing to the Internet router with IP address 1.1.1.2 as the next hop:

```
[edit]
```

```
root@host# set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.1/29
```

```
root@host# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.2
```

2. Enter the IP addresses of one or more DNS name servers. If your ISP does not support DHCP, then you might have to configure it statically.

```
[edit]
```

```
root@host# set system name-server 11.11.11.11
```



NOTE: The servers 208.67.222.222 and 208.67.222.220 are available as part of default configuration. You can add new servers or delete existing servers and configure new servers.

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)
- [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)
- [Validating the Branch SRX Series Configuration on page 19](#)
- [Verifying the Branch SRX Series Configuration on page 20](#)

Configuring a Network Time Protocol Server for the Branch SRX Series

Network Time Protocol (NTP) can be used to synchronize network devices to a common, and preferably accurate, time source. By synchronizing all network devices, timestamps on log messages are both accurate and meaningful.

1. Configure the NTP server and time zone.

```
[edit]
```

```
root@host# set system ntp server 160.90.182.55
```

```
[edit]
```

```
root@host# set system time-zone GMT-8
```

2. Update the system clock to make use of the new NTP server settings from operational mode.

```
root@host> set date NTP
```

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

- [Connecting the Branch SRX Series Through the Console Port for the First Time on page 15](#)
- [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)
- [Validating the Branch SRX Series Configuration on page 19](#)
- [Verifying the Branch SRX Series Configuration on page 20](#)

Validating the Branch SRX Series Configuration

Purpose Verify that the device was configured with a hostname, user classes, name server, and an NTP server.

Action From configuration mode, confirm your configuration by entering the **show** commands such as **show system host-name**, **show system login**, and **show system name-server** as shown in the following samples:

- Verify system hostname details.

```
[edit]
root@host# show system host-name
host-name srx210-host;
```

- Verify system user classes and login details.

```
[edit]
root@host# show system login
user admin-user {
  class super-user;
  authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
  }
}
user read-only-user {
  class read-only;
  authentication {
    encrypted-password "$A1B1C1"; ## SECRET-DATA
  }
}
```

- Verify system name server details.

```
[edit]
root@host# show system name-server
208.67.222.222;
208.67.220.220;
10.11.11.11
```

- Use **run show interface terse** to verify the acquired IP address.

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

Related Documentation • [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

- [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)
- [Configuring Internet Access for the Branch SRX Series on page 17](#)
- [Configuring a Network Time Protocol Server for the Branch SRX Series on page 18](#)
- [Verifying the Branch SRX Series Configuration on page 20](#)

Verifying the Branch SRX Series Configuration

Purpose Verify that your SRX Series configuration is working properly.

Action From configuration mode, confirm your configuration by entering the **show system services dhcp client** command.

- Verify DHCP client configuration.

```
user@srx210-host> show system services dhcp client ge-0/0/0.0
```

```
Logical Interface Name  ge-0/0/1.0
Hardware address       00:12:1e:a9:7b:81
Client Status          bound
Address obtained       1.1.1.20
update server          enables
Lease Obtained at      2007-05-10 18:16:04 PST
Lease Expires at       2007-05-11 18:16:04 PST
```

DHCP Options:

```
Name: name-server, Value: [ 1.1.1.2 ]
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [11.11.11.11]
Name: domain-name, Value: dept.example.net
```

- Verify the Internet connection on your SRX Series.
 - To verify the connectivity from your device, ping to the gateway and DNS from your SRX Series to verify the connectivity.
 - To verify that your SRX Series is connected and everything is working properly, access <http://www.juniper.net/techpubs/> or other Web destinations to ensure that you are connected to the Internet.

- Verify that the login classes you have created are working properly.

Log out from the device and log in again using the credentials that you have configured for the newly created user classes.

- Verify NTP server details.

```
user@srx210-host# show system ntp
server 160.90.182.55;
```

- Related Documentation**
- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
 - [Configuring a Hostname to Identify a Branch SRX Series Services Gateway in Your Network on page 16](#)
 - [Configuring Internet Access for the Branch SRX Series on page 17](#)
 - [Configuring a Network Time Protocol Server for the Branch SRX Series on page 18](#)
 - [Validating the Branch SRX Series Configuration on page 19](#)

Resetting the SRX Series Device

- [Resetting the Branch SRX Series on page 21](#)

Resetting the Branch SRX Series

Resetting Your Branch SRX Series

Resetting Your SRX Series to a Rescue Configuration

If someone accidentally commits an invalid configuration file, you can delete the invalid configuration and replace it with a previously stored rescue configuration.

To reset your services gateway to its rescue configuration, use a small probe, such as a straightened paperclip, to press and immediately release the **RESET CONFIG** button. Your services gateway will load and commit the rescue configuration. During this operation, the Status light on the front panel of your services gateway glows amber.

Resetting Your SRX Series to Factory Settings

If resetting your device to its rescue configuration does not resolve your access problem, you can reset your services gateway to its factory-default configuration, which deletes all previous configurations and loads the device's default settings.

To reset your services gateway to its factory-default configuration, use a small probe, such as a straightened paperclip, to press the **RESET CONFIG** button for 15 seconds or more.

- Related Documentation**
- [Connecting Your Branch SRX Series for the First Time](#)

CHAPTER 3

Configuring Basic SRX Series Features

- [Configuring Security Zones and Policies for SRX Series on page 23](#)
- [Configuring NAT for SRX Series on page 29](#)
- [Managing Licenses for SRX Series on page 35](#)
- [Configuring UTM for Branch SRX Series on page 36](#)
- [Configuring Intrusion Detection and Prevention for SRX Series on page 49](#)
- [Understanding Stateful Firewall, IPsec VPN, and Chassis Cluster for Branch SRX Series on page 55](#)

Configuring Security Zones and Policies for SRX Series

- [Understanding Security Zones and Policies for SRX Series on page 23](#)
- [Example: Configuring Security Zones and Policies for SRX Series on page 24](#)

Understanding Security Zones and Policies for SRX Series

This topic includes the following sections:

- [Zones on page 23](#)
- [Security Policy on page 24](#)

Zones

A zone is a collection of one or more network segments sharing identical security requirements. To group network segments within a zone, you must assign logical interfaces from the device to a zone.

Security zones are used to identify traffic flow direction in security policies to control traffic. On a single device, you can configure multiple security zones and at a minimum, you must define two security zones, basically to protect one area of the network from the other.

To configure the security zones, you must:

- Define zone (security or functional)
- Add logical interfaces to the zone

- Define permitted services (example: Telnet, SSH) and protocols (example: OSPF) destined to device itself.

Default configuration of the branch SRX Series includes two security zones--trust and untrust. The vlan.0 belongs to the trust zone and ge-0/0/0 belongs to the untrust zone.

For more details on security zones, see *Building Blocks Feature Guide for Security Devices*.

Security Policy

A security policy is a set of statements, or rules, that controls traffic from a specified source (source-address and optionally source-identity) to a specified destination (destination-address) using a specified service (application). If the SRX Series device receives a packet that matches the specifications of one of the rules in the security policy, the SRX Series performs on the packet the action defined by that policy rule.

[Table 7 on page 24](#) provides details of factory default settings for security policies on branch SRX Series devices.

Table 7: Factory-Default Settings for Security Policies for Branch SRX Series Devices

From Zone	To Zone	Action
Trust zone	Untrust zone	Allow
Trust zone	Trust zone	Allow
Untrust zone	Trust zone	Deny

For more details on security policies, see *Building Blocks Feature Guide for Security Devices*.

Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Connecting Your Branch SRX Series for the First Time](#)
- [Example: Configuring Security Zones and Policies for SRX Series on page 24](#)

Example: Configuring Security Zones and Policies for SRX Series

This example shows how to set up a new zone and add three application servers to that zone. Then you provide communication between a host (PC) in the trust zone to the servers in the newly created zone and also facilitate communication between two servers within the zone.

To meet this requirement, you need an interzone security policy to allow traffic between two zones and an intrazone policy to allow traffic between servers within a zone.

Requirements

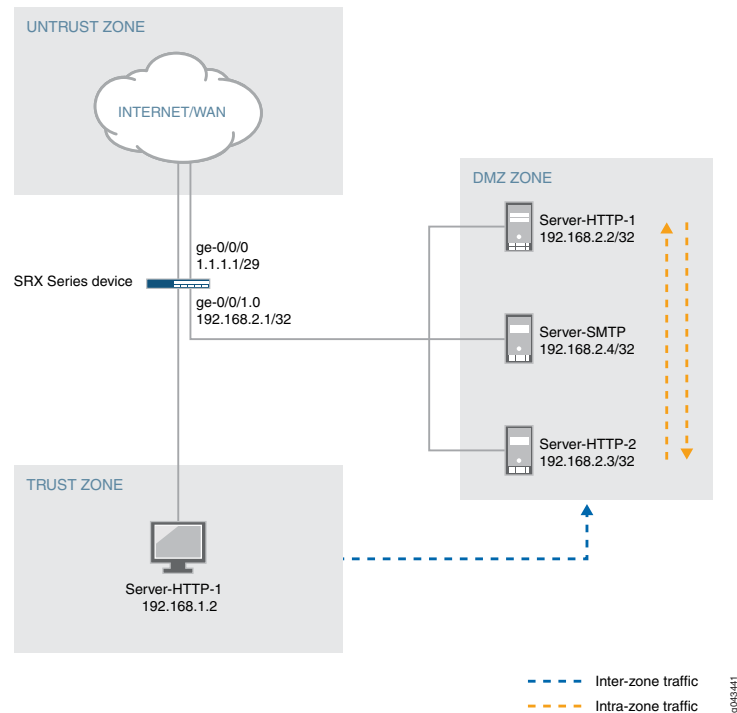
This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

Overview

This example uses the network topology shown in [Figure 3 on page 25](#).

Figure 3: Topology for Security Policy Configuration



In this example, you perform the following tasks:

- Move the ge-0/0/1.0 interface, which was part of trust zone, to the DMZ zone and assign IP address 192.168.2.1/24. Change ge-0/0/1 from family ethernet-switching (factory configuration setting) to family inet.
- Assign IP address 192.168.1.2/24 to the host connected to the fe-0/0/2.0 interface in the trust zone.
- Set up two HTTP servers (Server-HTTP-1 and Server-HTTP-2) and one SMTP server and assign IP addresses 192.168.2.2/24, 192.168.2.3/24, and 192.168.2.4/24 respectively in the DMZ zone.
- Configure an address book and create addresses for use in the policy as shown in [Table 8 on page 26](#).

Table 8: Address Books Configuration

Zones	Address Book	Server IP Address-
DMZ	Server-HTTP-1	192.168.2.2/24
	Server-HTTP-2	192.168.2.3/24
	Server-SMTP	192.168.2.4/24
Trust	PC-Trust	192.168.1.2/24

- Create security policies as shown in [Table 9 on page 26](#).

Table 9: Security Policy Configuration

Policy Name	From Zone	To Zone	Action
permit-mail-trust-DMZ	Trust	DMZ	Permit SMTP traffic
permit-http-in-DMZ	DMZ	DMZ	Permit HTTP traffic

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.

```
delete interfaces ge-0/0/1 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family inet address 192.168.2.1/24
set security zones security-zone DMZ interfaces ge-0/0/1 host-inbound-traffic
system-services all
set security zones security-zone DMZ address-book address Server-HTTP-1 192.168.2.2/24
set security zones security-zone DMZ address-book address Server-HTTP-2 192.168.2.3/24
set security zones security-zone DMZ address-book address Server-SMTP 192.168.2.4/24
set security zones security-zone DMZ address-book address-set DMZ-address-set-http
address Server-HTTP-1
set security zones security-zone DMZ address-book address-set DMZ-address-set-http
address Server-HTTP-2
set security zones security-zone trust address-book address PC-Trust 192.168.1.2/32
set security policies from-zone trust to-zone DMZ policy permit-mail-trust-DMZ match
source-address PC-Trust
set security policies from-zone trust to-zone DMZ policy permit-mail-trust-DMZ match
destination-address Server-SMTP
set security policies from-zone trust to-zone DMZ policy permit-mail-trust-DMZ match
application junos-smtp
set security policies from-zone trust to-zone DMZ policy permit-mail-trust-DMZ then
permit
set security policies from-zone DMZ to-zone DMZ policy permit-http-in-DMZ match
source-address DMZ-address-set-http
set security policies from-zone DMZ to-zone DMZ policy permit-http-in-DMZ match
destination-address DMZ-address-set-http
```



```

set security policies from-zone DMZ to-zone DMZ policy permit-http-in-DMZ match
  application junos-http
set security policies from-zone DMZ to-zone DMZ policy permit-http-in-DMZ then permit

```

To configure security zones and policies:

1. Delete the interface ge-0/0/1 from family ethernet-switching (factory configuration) and assign an IP address.

```

[edit]
user@srx210-host# delete interfaces ge-0/0/1 unit 0 family ethernet-switching
user@srx210-host# set interfaces ge-0/0/1 unit 0 family inet address 192.168.2.1/24

```

2. Configure a new security zone (DMZ) and assign interfaces.

```

[edit]
user@srx210-host# set security zones security-zone DMZ interfaces ge-0/0/1
  host-inbound-traffic system-services all

```

3. Create address books in the DMZ zone.

```

[edit]
user@srx210-host# set security zones security-zone DMZ address-book address
  Server-HTTP-1 192.168.2.2/32
user@srx210-host# set security zones security-zone DMZ address-book address
  Server-HTTP-2 192.168.2.3/32
user@srx210-host# set security zones security-zone DMZ address-book address
  Server-SMTP 192.168.2.4/32

```

4. Create address sets in the DMZ zone to group HTTP server addresses together.

```

[edit]
user@srx210-host# set security zones security-zone DMZ address-book address-set
  DMZ-address-set-http address Server-HTTP-1
user@srx210-host# set security zones security-zone DMZ address-book address-set
  DMZ-address-set-http address Server-HTTP-2

```

5. Create address books in the trust zone.

```

[edit]
user@srx210-host# set security zones security-zone trust address-book address
  PC-Trust 192.168.1.2/32

```

6. Create an interzone policy to permit SMTP traffic from the trust zone to the DMZ zone.

```

[edit]
user@srx210-host# set security policies from-zone trust to-zone DMZ policy
  permit-mail-trust-DMZ match source-address PC-Trust
user@srx210-host# set security policies from-zone trust to-zone DMZ policy
  permit-mail-trust-DMZ match destination-address Server-SMTP
user@srx210-host# set security policies from-zone trust to-zone DMZ policy
  permit-mail-trust-DMZ match application junos-smtp
user@srx210-host# set security policies from-zone trust to-zone DMZ policy
  permit-mail-trust-DMZ then permit

```

7. Create an intrazone policy to permit HTTP traffic between the two servers in the DMZ zone.

```

[edit]

```

```
user@srx210-host# set security policies from-zone DMZ to-zone DMZ policy
  permit-http-in-DMZ match source-address DMZ-address-set-http
user@srx210-host# set security policies from-zone DMZ to-zone DMZ policy
  permit-http-in-DMZ match destination-address DMZ-address-set-http
user@srx210-host# set security policies from-zone DMZ to-zone DMZ policy
  permit-http-in-DMZ match application junos-http
user@srx210-host# set security policies from-zone DMZ to-zone DMZ policy
  permit-http-in-DMZ then permit
```

Results From configuration mode, confirm your configuration by entering the **show security zones** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@srx210-host# show security zones security-zone DMZ
address-book {
  address Server-HTTP-1 192.168.2.2/24;
  address Server-HTTP-2 192.168.2.3/24;
  address Server-SMTP 192.168.2.4/24;
  address-set DMZ-address-set-http {
    address Server-HTTP-1;
    address Server-HTTP-2;
  }
}
interfaces {
  ge-0/0/1.0 {
    host-inbound-traffic {
      system-services {
        all;
      }
    }
  }
}

[edit]
user@srx210-host# show security policies from-zone trust to-zone DMZ
policy permit-mail-trust-DMZ {
  match {
    source-address PC-Trust;
    destination-address Server-SMTP;
    application junos-smtp;
  }
  then {
    permit;
  }
}

[edit]
user@srx210-host# show security policies from-zone DMZ to-zone DMZ
policy permit-http-in-DMZ {
  match {
    source-address DMZ-address-set-http;
    destination-address DMZ-address-set-http;
    application junos-http;
  }
}
```

```

    then {
      permit;
    }
  }
}

```

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

Verification

Verifying Policy Configuration

Purpose Verify information about security policies.

Action You can pass traffic between servers in different zones and verify the traffic data by using the **show security flow session** command from operational mode.

For samples of the **show security flow session** command output, see [show security flow session](#).

Related Documentation

- [Understanding Security Zones and Policies for SRX Series on page 23](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Connecting Your Branch SRX Series for the First Time](#)

Configuring NAT for SRX Series

- [Understanding NAT for SRX Series on page 29](#)
- [Example: Configuring Destination NAT for SRX Series on page 30](#)

Understanding NAT for SRX Series

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either of the source and destination addresses or both addresses in a packet can be translated. NAT can include the translation of IP addresses as well as port numbers.

The following types of NAT are supported on an SRX Series:

- **Static NAT**—Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction.

Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size.

- **Destination NAT**—Destination NAT is the translation of the destination IP address of a packet entering the SRX Series. Destination NAT is used to redirect traffic destined to a virtual host (identified by the original destination IP address) to the real host (identified by the translated destination IP address).

In general, destination NAT allows connections to be initiated for incoming network connections—for example, from the Internet to a private network.

- **Source NAT**—Source NAT is the translation of the source IP address of a packet leaving the SRX Series. Source NAT is used to allow hosts with private IP addresses to access a public network. On the SRX210, source NAT from the trust to the untrust zone is enabled by default.

In general, source NAT allows connections to be initiated for outgoing network connections—for example, from a private network to the Internet.

For more information, see the *Network Address Translation Feature Guide for Security Devices*.

**Related
Documentation**

- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)
- [Connecting Your Branch SRX Series for the First Time](#)
- [Example: Configuring Destination NAT for SRX Series on page 30](#)

Example: Configuring Destination NAT for SRX Series

Before you can get access to your internal network from the outside, you need to configure destination NAT. In this example, you are applying destination NAT to allow connections from the Internet to a private network (in the DMZ zone) after translating the public IP address to the private address.

Requirements

Before you begin, create security zones and assign interfaces to them. See [“Example: Configuring Security Zones and Policies for SRX Series” on page 24](#).

This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

Overview

Using the topology shown in [Figure 4 on page 31](#), you are applying destination NAT to the traffic destined to 1.1.1.3 coming from the untrust zone. This traffic should be translated into the private IP address of 192.168.2.2 as shown in [Table 10 on page 31](#).

Figure 4: Destination NAT Single Address Translation

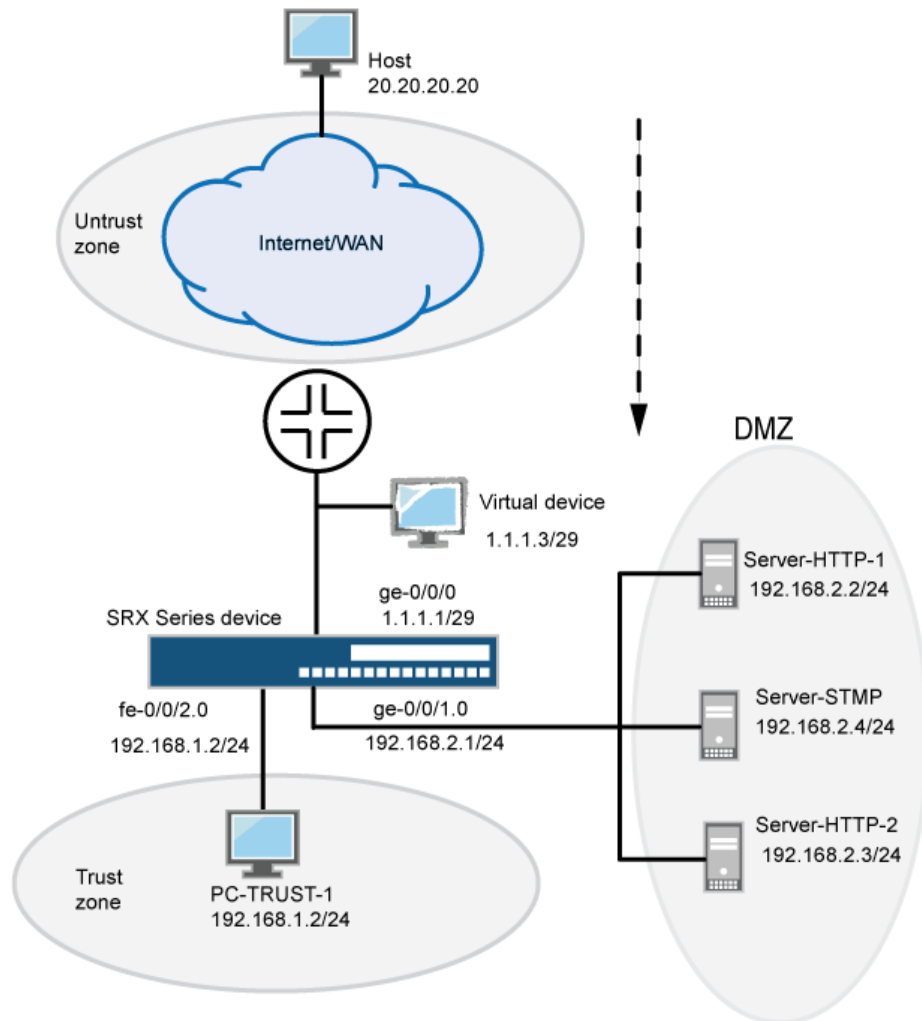


Table 10: Destination NAT Mapping

Before Translation		After Translation	
Source IP Address	Destination IP Address	Source IP Address	Translated Destination IP Address
20.20.20.20	1.1.1.3	1.1.1.3	192.168.2.2

In this topology, you provide access to the server (Server-HTTP-1) in the DMZ zone from the Internet after translating the public IP address 1.1.1.3 to the private address 192.168.2.2 and forward traffic to the internal network if the request is coming from ge-0/0/0.0.

In this example, you perform the following tasks:

- Create a destination NAT pool called `dst-nat-pool-1` to include the IP address 192.168.2.2.
- Create a destination NAT rule set `rs1`, where rule `r1` matches the packets received from the `ge-0/0/0.0` interface with the destination IP address 1.1.1.3. For matching packets, the destination address is translated to the address in the `dst-nat-pool-1` pool.
- Use an existing address book (as applicable) or create a new address book for `Server-HTTP-1`.
- Configure traffic from the untrust zone with a destination address of 1.1.1.3 to be translated to the private address 192.168.2.2 in the DMZ zone.
- Configure the device to respond to proxy ARP for the addresses in the IP pool.
- Create a security policy to permit HTTP traffic from the untrust zone to the DMZ zone.



NOTE: Because the destination NAT rule sets are evaluated before a security policy, the address referred to in the security policy must be the real IP address of the end host.

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 nat destination pool dst-nat-pool-1 address 192.168.2.2/32
set security nat destination rule-set rs1 from interface ge-0/0/0.0
set security nat destination rule-set rs1 rule r1 match destination-address 1.1.1.3/29
set security nat destination rule-set rs1 rule r1 then destination-nat pool dst-nat-pool-1
set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.3/29
set security zones security-zone DMZ address-book address Server-HTTP-1 192.168.2.2/32
set security policies from-zone untrust to-zone DMZ policy server-access match
  source-address any
set security policies from-zone untrust to-zone DMZ policy server-access match
  destination-address Server-HTTP-1
set security policies from-zone untrust to-zone DMZ policy server-access match application
  junos-http
set security policies from-zone untrust to-zone DMZ policy server-access then permit
```

To configure a destination NAT rule:

1. Create the destination NAT pool to include the IP address of the server (`Server-HTTP-1`).

```
[edit]
user@srx210-host# set security nat destination pool dst-nat-pool-1 address
192.168.2.2/32
```

2. Create a destination NAT rule set.

```
[edit]
user@srx210-host# set security nat destination rule-set rs1 from interface ge-0/0/0.0
```

3. Configure a rule that matches packets and translates the destination address (1.1.1.3/29) to the address in the pool (dst-nat-pool-1 that includes IP address 192.168.2.2/32).

```
[edit]
user@srx210-host# set security nat destination rule-set rs1 rule r1 match
destination-address 1.1.1.3/29
user@srx210-host# set security nat destination rule-set rs1 rule r1 then destination-nat
pool dst-nat-pool-1
```

4. Configure proxy ARP for the address 1.1.1.3/29 on interface ge-0/0/0.0.

```
[edit]
user@srx210-host# set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.3/29
```

5. Configure an address in the address book for Server-HTTP-1.

```
[edit]
user@srx210-host# edit security zones security-zone DMZ address-book address
Server-HTTP-1 192.168.2.2/32
```

6. Configure a security policy to allow traffic from the untrust zone to the server (Server-HTTP-1) in the DMZ zone.

```
[edit]
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
server-access match source-address any
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
server-access match destination-address Server-HTTP-1
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
server-access match application junos-http
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
server-access then permit
```

Results From configuration mode [edit], confirm your configuration by entering the **show security nat destination** and **show security policies from-zone untrust to-zone DMZ** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@srx210-host# show security nat destination
pool dst-nat-pool-1 {
    address 192.168.2.2/32;
}
rule-set rs1 {
    from interface ge-0/0/0.0;
    rule r1 {
        match {
            destination-address 1.1.1.3/29;
        }
        then {
            destination-nat {
                pool {
                    dst-nat-pool-1;
                }
            }
        }
    }
}
```

```

    }
  }

[edit]
user@srx210-host# show security policies from-zone untrust to-zone DMZ
policy server-access {
  match {
    source-address any;
    destination-address Server-HTTP-1;
    application junos-http;
  }
  then {
    permit;
  }
}

```

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

Verification

Confirm that the configuration is working properly.

- [Verify the Destination NAT Rule on page 34](#)
- [Verifying NAT Application to Traffic on page 34](#)

Verify the Destination NAT Rule

Purpose Verify that there is traffic using IP addresses from the destination NAT pool.

Action From operational mode, enter the **show security nat destination summary** command. View the translation hits field to check for traffic using IP addresses from the pool.

```

Total pools: 1
Pool name      Address                               Routing      Port  Total
dst-nat-pool-1 Range
                192.168.2.2 - 192.168.2.2 Instance    Address
                default          0          1

Total rules: 1
Rule name      Rule set      From          Action
r1             rs1           ge-0/0/0.0
dst-nat-pool-1

```

Meaning Displays a summary of NAT destination pool information.

Verifying NAT Application to Traffic

Purpose Verify that NAT is being applied to the specified traffic.

Action From operational mode, enter the **show security flow session** command to display information about all currently active security sessions on the device.

Related Documentation

- [Understanding NAT for SRX Series on page 29](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 5](#)

- *Connecting Your Branch SRX Series for the First Time*

Managing Licenses for SRX Series

- [Updating Licenses for a Branch SRX Series on page 35](#)

Updating Licenses for a Branch SRX Series

You need to install a license for some of the advanced security features such as UTM and IDP on a branch SRX Series.

Licensing is usually ordered when the device is purchased, and this information is bound to the chassis serial number. These instructions assume that you already have the license. If you have not ordered the licenses during the purchase of the device, contact your account team or Juniper customer care for assistance.

For more information, refer to the Knowledge Base article KB9731 at <http://kb.juniper.net/KB9731>.

You can install the license on the SRX Series using either the automatic method or manual method as follows:

- Install your license automatically on the device

To install or update your license automatically, your device must be connected to the Internet.

```
user@srx210-host> request system license update
```

Trying to update license keys from <https://ae1.juniper.net>, use 'show system license' to check status.

- Install the licenses manually on the device.

```
user@srx210-host> request system license add terminal
```

[Type ^D at a new line to end input,
enter blank line between each license key]

Paste the license key and press Enter to continue.

To verify the license installed on your system, use the **show system license command** as shown in the following examples:

- View license usage:

Feature name	Licenses	Licenses used	Expiry installed	needed	
av_key_kaspersky_engine	0	1	0	2013-12-31	
08:00:00 GMT-8					
avs	0	1	0	2013-12-31	
08:00:00 GMT-8					
anti_spam_key_sb1	0	2	0	2013-12-31	
08:00:00 GMT-8					
wf_key_surfcontrol_cpa	0	2	0	2013-12-31	
08:00:00 GMT-8					
idp-sig	0	2	0	2013-12-31	
08:00:00 GMT-8					

ax411-wlan-ap	0	2	0	permanent
av_key_sophos_engine	1	0	1	3 days
logical-system	0	1	0	permanent

The output sample is truncated to display only license usage details.

- View license details for IDP:

```
License identifier: JUNOS240192
License version: 2
Valid for device: AH1111AA7883
Features:
  idp-sig          - IDP Signature
  date-based, 2010-01-04 08:00:00 GMT-8 - 2013-12-31 08:00:00 GMT-8
```

The output sample is truncated to display only the IDP license.

- View license usage for UTM features:

```
License identifier: JUNOS240185
License version: 2
Valid for device: AH1111AA7883
Features:
  av_key_kaspersky_engine - Kaspersky AV
  date-based, 2010-01-04 08:00:00 GMT-8 - 2013-12-31 08:00:00 GMT-8
```

```
License identifier: JUNOS240186
License version: 2
Valid for device: AH1111AA7883
Features:
  anti_spam_key_sb1 - Anti-Spam
  date-based, 2010-01-04 08:00:00 GMT-8 - 2013-12-31 08:00:00 GMT-8
```

```
License identifier: JUNOS240187
License version: 2
Valid for device: AH1111AA7883
Features:
  wf_key_surfcontrol_cpa - Web Filtering
  date-based, 2010-01-04 08:00:00 GMT-8 - 2013-12-31 08:00:00 GMT-8
```

The output sample is truncated to display some of the UTM features license.

- Related Documentation**
- [request system license update on page 90](#)
 - [show system license \(View\) on page 115](#)

Configuring UTM for Branch SRX Series

- [Understanding Unified Threat Management for Branch SRX Series on page 37](#)
- [Example: Configuring Unified Threat Management for a Branch SRX Series on page 38](#)
- [Default UTM Policy for Branch SRX Series on page 42](#)
- [Predefined UTM Profile Configuration for Branch SRX Series on page 42](#)

Understanding Unified Threat Management for Branch SRX Series

Unified Threat Management (UTM) is an optional function for the branch SRX Series that provides an integrated suite of network security features to protect against multiple threat types including spam and phishing attacks, viruses, trojans and spyware infected files, unapproved website access, and unapproved content.

With UTM, you can implement a comprehensive set of security features that include antispam, antivirus, Web filtering, and content filtering protection.

The UTM features provide the ability to prevent threats at the SRX Series device before the threats enter the network.

The following UTM modules are supported:

- **Antispam**—Antispam blocks and filters unwanted e-mail traffic by scanning inbound and outbound SMTP e-mail traffic by using some combination of spam block lists (SBL) and user-configured blacklists and whitelists.
- **Antivirus**—Antivirus feature uses an integrated scanning engine and virus signature databases to protect against viruses, trojans, rootkits, worms, and other types of malicious code from reaching devices on your network.
- **Web filtering**—Web filtering allows you to permit or block access to specific websites individually or based on the categories to which the website belongs.
- **Content filtering**—Content filtering provides basic data loss prevention functionality. Content filtering filters traffic based on MIME type, file extension, and protocol commands.

The SRX Series has predefined system profiles (antispam, antivirus, or Web filtering) designed to provide basic protection. You can use a predefined profile to bind to the UTM policy or you can also create a component (antispam, antivirus, Web filtering, or content filtering) profile.

[Table 11 on page 37](#) provides UTM modules, feature profiles, and supported protocol details.

Table 11: Default UTM Profiles on Branch SRX Series

UTM Modules	Categories	Types	Default Profiles	Supported Protocols
Antispam	NA	smtp-profile	junos-as-defaults	SMTP
Antivirus	Full antivirus	kaspersky-lab-engine	junos-av-defaults	SMTP, POP3, IMAP, HTTP and FTP
	Express antivirus	juniper-express-engine	junos-eav-defaults	
	Sophos antivirus	sophos-engine	junos-sophos-av-defaults	

Table 11: Default UTM Profiles on Branch SRX Series (*continued*)

UTM Modules	Categories	Types	Default Profiles	Supported Protocols
Web filtering	Integrated Web filtering	surf-control-integrated	junos-wf-cpa-default	HTTP
	Redirect Web filtering	websense-redirect	junos-wf-websense-default	
	Local Web filtering	juniper-local	junos-wf-local-default	
	Enhanced Web filtering	juniper-enhanced	junos-wf-enhanced-default	
Content filtering	NA	NA	NA	SMTP, POP3, IMAP, HTTP, and FTP

To enable UTM on your SRX Series , you must:

- Install UTM licenses (See [“Updating Licenses for a Branch SRX Series” on page 35.](#))
- Create UTM profiles for UTM components (antispam, antivirus, content filtering, and Web filtering)
- Map a UTM profile to a UTM policy
- Map a UTM policy to a security policy

For more details on UTM, see *UTM Feature Guide for Security Devices*.

- Related Documentation**
- [Updating Licenses for a Branch SRX Series on page 35](#)
 - [Example: Configuring Unified Threat Management for a Branch SRX Series on page 38](#)

Example: Configuring Unified Threat Management for a Branch SRX Series

This example shows how to configure UTM quickly on your branch SRX Series by using the predefined UTM components.

Requirements

Before you begin, install or verify a UTM feature license. See [“Updating Licenses for a Branch SRX Series” on page 35.](#)

This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

Overview

In this example, you enable UTM components (antispam, antivirus, and Web filtering) on the SRX210 by applying the following preconfigured profiles:

- Antispam protection by using the junos-as-defaults profile to block and filter spam e-mail messages.
- Antivirus protection by using the junos-av-defaults profile to detect and block malicious codes.
- Web filtering by using the junos-wf-cpa-default profile to block access to (HTTP) websites based on IP address or URL.

After you create a UTM policy, attach the UTM policy to the default security policy.

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 utm utm-policy policy-utm-all anti-spam smtp-profile junos-as-defaults
set security utm utm-policy policy-utm-all anti-virus http-profile junos-av-defaults
set security utm utm-policy policy-utm-all web-filtering http-profile junos-wf-cpa-default
set security policies from-zone trust to-zone untrust policy trust-to-untrust match
source-address any destination-address any application any
set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit
application-services utm-policy policy-utm-all
```

Step-by-Step Procedure

To configure UTM components:

1. Create a UTM policy and apply the default antispam profile to the UTM policy.

```
[edit]
user@srx210-host# set security utm utm-policy policy-utm-all anti-spam
smtp-profile junos-as-defaults
```

2. Attach a predefined antivirus profile for the HTTP protocol to the UTM policy.

```
[edit]
user@srx210-host# set security utm utm-policy policy-utm-all anti-virus http-profile
junos-av-defaults
```



NOTE: A separate antivirus profile is required for each protocol. The available protocols include HTTP, SMTP, POP3, and IMAP.

3. Attach a predefined Web filtering profile for HTTP to the UTM policy.

```
[edit]
user@srx210-host# set security utm utm-policy policy-utm-all web-filtering
http-profile junos-wf-cpa-default
```

4. Attach the UTM policy to the default security policy (policy from the trust zone to the untrust zone), and set the application services to be allowed.

```
[edit]
user@srx210-host# set security policies from-zone trust to-zone untrust policy
trust-to-untrust match source-address any destination-address any application
any
user@srx210-host# set security policies from-zone trust to-zone untrust policy
trust-to-untrust then permit application-services utm-policy policy-utm-all
```

Results From configuration mode, confirm your configuration by entering the **show security utm** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@srx210-host# show security utm
utm-policy policy-utm-all {
  anti-virus {
    http-profile junos-av-defaults;
  }
  web-filtering {
    http-profile junos-wf-cpa-default;
  }
  anti-spam {
    smtp-profile junos-as-defaults;
  }
}

[edit]
user@srx210-host# show security policies from-zone trust to-zone untrust policy
trust-to-untrust
policy trust-to-untrust {
  match {
    source-address any;
    destination-address any;
    application any;
  }
  then {
    permit {
      application-services {
        utm-policy policy-utm-all;
      }
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying Web Filtering Status on page 41](#)
- [Verifying Antispam Status on page 41](#)
- [Verifying Antivirus Protection on page 41](#)

Verifying Web Filtering Status

Purpose Verify that the Web filtering status configuration is working properly.

Action From operational mode, enter the **show security utm web-filtering status** command.

```
user@srx210-host# show security utm web-filtering status
```

```
UTM web-filtering status:
  Server status: SC-CPA server up
```

Verifying Antispam Status

Purpose Verify that the antispam filtering configuration is active.

Action From operational mode, enter the **show security utm anti-spam status** command.

```
user@srx210-host>show security utm anti-spam status
```

```
SBL Whitelist Server:
SBL Blacklist Server:
  msgsecurity.example.net

DNS Server:
  Primary   : 208.67.222.222, Src Interface: ge-0/0/0
  Secondary : 208.67.220.220, Src Interface: ge-0/0/1
  Ternary   : 10.189.132.70, Src Interface: fe-0/0/2
```

Verifying Antivirus Protection

Purpose Verify that the antivirus protection configuration is working properly.

Action From operational mode, enter the **show security utm anti-virus status** command.

```
user@srx210-host>show security utm anti-virus status
```

```
UTM anti-virus status:

Anti-virus key expire date: 2010-12-31 00:00:00
Update server: http://update.juniper-updates.net/AV/SRX210
Interval: 120 minutes
Pattern update status: next update in 54 minutes
Last result: already have latest database
Anti-virus signature version: 09/03/2009 07:01 GMT-8, virus records: 467973
Anti-virus signature compiler version: N/A
Scan engine type: kaspersky-lab-engine
Scan engine information: last action result: No error(0x00000000)
```

- Related Documentation**
- [Updating Licenses for a Branch SRX Series on page 35](#)
 - [Understanding Unified Threat Management for Branch SRX Series on page 37](#)
 - [Predefined UTM Profile Configuration for Branch SRX Series on page 42](#)
 - [Default UTM Policy for Branch SRX Series on page 42](#)

Default UTM Policy for Branch SRX Series

Default UTM Policy

```
anti-virus {  
  http-profile junos-av-defaults;  
  ftp {  
    upload-profile junos-av-defaults;  
    download-profile junos-av-defaults;  
  }  
  smtp-profile junos-av-defaults;  
  pop3-profile junos-av-defaults;  
  imap-profile junos-av-defaults;  
}  
web-filtering {  
  http-profile junos-wf-cpa-default;  
}
```

- Related Documentation**
- [Understanding Unified Threat Management for Branch SRX Series on page 37](#)
 - [Example: Configuring Unified Threat Management for a Branch SRX Series on page 38](#)

Predefined UTM Profile Configuration for Branch SRX Series

This topic includes the following sections:

- [Antispam on page 42](#)
- [Antivirus on page 42](#)
- [Web Filtering on page 44](#)

Antispam

```
sbl {  
  profile junos-as-defaults {  
    sbl-default-server;  
    spam-action block;  
    custom-tag-string ***SPAM***;  
  }  
}
```

Antivirus

```
kaspersky-lab-engine {  
  pattern-update {  
    url http://update.juniper-updates.net/AV/SRX210/;  
    interval 60;  
  }  
}
```



```
profile junos-av-defaults {
  fallback-options {
    default log-and-permit;
    corrupt-file log-and-permit;
    password-file log-and-permit;
    decompress-layer log-and-permit;
    content-size log-and-permit;
    engine-not-ready log-and-permit;
    timeout log-and-permit;
    out-of-resources log-and-permit;
    too-many-requests log-and-permit;
  }
  scan-options {
    intelligent-prescreening;
    scan-mode all;
    content-size-limit 10000;
    timeout 180;
    decompress-layer-limit 2;
  }
  notification-options {
    virus-detection {
      type message;
      no-notify-mail-sender;
      custom-message "VIRUS WARNING";
    }
    fallback-block {
      type message;
      no-notify-mail-sender;
    }
  }
}

juniper-express-engine {
  pattern-update {
    url http://update.juniper-updates.net/EAV/SRX210/;
    interval 1440;
  }
  profile junos-eav-defaults {
    fallback-options {
      default log-and-permit;
      content-size log-and-permit;
      engine-not-ready log-and-permit;
      timeout log-and-permit;
      out-of-resources log-and-permit;
      too-many-requests log-and-permit;
    }
    scan-options {
      intelligent-prescreening;
      content-size-limit 10000;
      timeout 180;
    }
    notification-options {
      virus-detection {
        type message;
        no-notify-mail-sender;
        custom-message "VIRUS WARNING";
      }
    }
  }
}
```

```
    }
    fallback-block {
        type message;
        no-notify-mail-sender;
    }
}
}
sophos-engine {
    pattern-update {
        url http://update.juniper-updates.net/SAV/;
        interval 1440;
    }
    profile junos-sophos-av-defaults {
        fallback-options {
            default log-and-permit;
            content-size log-and-permit;
            engine-not-ready log-and-permit;
            timeout log-and-permit;
            out-of-resources log-and-permit;
            too-many-requests log-and-permit;
        }
        scan-options {
            uri-check;
            content-size-limit 10000;
            timeout 180;
        }
        notification-options {
            virus-detection {
                type message;
                no-notify-mail-sender;
                custom-message "VIRUS WARNING";
            }
            fallback-block {
                type message;
                no-notify-mail-sender;
            }
        }
    }
}
```

Web Filtering

```
surf-control-integrated {
    server {
        host cpa.surfcpa.com;
        port 9020;
    }
    profile junos-wf-cpa-default {
        category {
            Adult_Sexually_Explicit {
                action block;
            }
            Advertisements {
                action block;
            }
        }
    }
}
```

```
Arts_Entertainment {  
    action permit;  
}  
Chat {  
    action permit;  
}  
Computing_Internet {  
    action permit;  
}  
Criminal_Skills {  
    action block;  
}  
Drugs_Alcohol_Tobacco {  
    action block;  
}  
Education {  
    action permit;  
}  
Finance_Investment {  
    action permit;  
}  
Food_Drink {  
    action permit;  
}  
Gambling {  
    action block;  
}  
Games {  
    action block;  
}  
Glamour_Intimate_Apparel {  
    action permit;  
}  
Government_Politics {  
    action permit;  
}  
Hacking {  
    action block;  
}  
Hate_Speech {  
    action block;  
}  
Health_Medicine {  
    action permit;  
}  
Hobbies_Recreation {  
    action permit;  
}  
Hosting_Sites {  
    action permit;  
}  
Job_Search_Career_Development {  
    action permit;  
}  
Kids_Sites {  
    action permit;
```

```
}
Lifestyle_Culture {
    action permit;
}
Motor_Vehicles {
    action permit;
}
News {
    action permit;
}
Personals_Dating {
    action block;
}
Photo_Searches {
    action permit;
}
Real_Estate {
    action permit;
}
Reference {
    action permit;
}
Religion {
    action permit;
}
Remote_Proxies {
    action block;
}
Sex_Education {
    action block;
}
Search_Engines {
    action permit;
}
Shopping {
    action permit;
}
Sports {
    action permit;
}
Streaming_Media {
    action permit;
}
Travel {
    action permit;
}
Usenet_News {
    action permit;
}
Violence {
    action block;
}
Weapons {
    action block;
}
Web_based_Email {
```

```

        action permit;
    }
}
default log-and-permit;
custom-block-message "Juniper Web Filtering has been set to block this site.";
fallback-settings {
    default log-and-permit;
    server-connectivity log-and-permit;
    timeout log-and-permit;
    too-many-requests log-and-permit;
}
}
}
websense-redirect {
    profile junos-wf-websense-default {
        custom-block-message "Juniper Web Filtering has been set to block this site.";
        fallback-settings {
            default log-and-permit;
            server-connectivity log-and-permit;
            timeout log-and-permit;
            too-many-requests log-and-permit;
        }
    }
}
juniper-local {
    profile junos-wf-local-default {
        custom-block-message "Juniper Web Filtering has been set to block this site.";
        fallback-settings {
            default log-and-permit;
            server-connectivity log-and-permit;
            timeout log-and-permit;
            too-many-requests log-and-permit;
        }
    }
}
juniper-enhanced {
    server {
        host rp.cloud.threatseeker.com;
        port 80;
    }
    profile junos-wf-enhanced-default {
        category {
            Enhanced_Adult_Material {
                action block;
            }
            Enhanced_Gambling {
                action block;
            }
            Enhanced_Games {
                action block;
            }
            Enhanced_Illegal_or_Questionable {
                action block;
            }
            Enhanced_Tasteless {
                action block;
            }
        }
    }
}

```

```
}
Enhanced_Violence {
    action block;
}
Enhanced_Weapons {
    action block;
}
Enhanced_Militancy_and_Extremist {
    action block;
}
Enhanced_Racism_and_Hate {
    action block;
}
Enhanced_Advertisements {
    action block;
}
Enhanced_Nudity {
    action block;
}
Enhanced_Adult_Content {
    action block;
}
Enhanced_Sex {
    action block;
}
Enhanced_Hacking {
    action block;
}
Enhanced_Personals_and_Dating {
    action block;
}
Enhanced_Alcohol_and_Tobacco {
    action block;
}
Enhanced_Abused_Drugs {
    action block;
}
Enhanced_Marijuana {
    action block;
}
Enhanced_Malicious_Web_Sites {
    action block;
}
Enhanced_Spyware {
    action block;
}
Enhanced_Phishing_and_Other_Frauds {
    action block;
}
Enhanced_Keyloggers {
    action block;
}
Enhanced_Emerging_Exploits {
    action block;
}
Enhanced_Potentially_Damaging_Content {
```

```

        action block;
    }
    Enhanced_Malicious_Embedded_Link {
        action block;
    }
    Enhanced_Malicious_Embedded_iFrame {
        action block;
    }
    Enhanced_Suspicious_Embedded_Link {
        action block;
    }
}
default log-and-permit;
custom-block-message "Juniper Web Filtering has been set to block this site.";
fallback-settings {
    default log-and-permit;
    server-connectivity log-and-permit;
    timeout log-and-permit;
    too-many-requests log-and-permit;
}
}
}

```

- Related Documentation**
- [Understanding Unified Threat Management for Branch SRX Series on page 37](#)
 - [Example: Configuring Unified Threat Management for a Branch SRX Series on page 38](#)

Configuring Intrusion Detection and Prevention for SRX Series

- [Understanding Intrusion Detection and Prevention for SRX Series on page 49](#)
- [Example: Configuring Intrusion Detection and Prevention for SRX Series on page 50](#)

Understanding Intrusion Detection and Prevention for SRX Series

An Intrusion Detection and Prevention (IDP) policy lets you selectively enforce various attack detection and prevention techniques on the network traffic passing through your SRX Series. The SRX Series offer the same set of IDP signatures that are available on Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to secure networks against attacks. The basic IDP configuration involves the following tasks:

- Download and install the IDP license—See [“Updating Licenses for a Branch SRX Series” on page 35](#).
- Download and install the signature database—You must download and install the IDP signature database. The signature databases are available as a security package on the Juniper Networks website. This database includes attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.
- Configure recommended policy as the IDP policy—Juniper Networks provides predefined policy templates to use as a starting point for creating your own policies. Each template is a set of rules of a specific rulebase type that you can copy and then update according to your requirements.

To get started, we recommend you use the predefined policy named “Recommended”.

- Enable a security policy for IDP inspection—For transit traffic to pass through IDP inspection, you configure a security policy and enable IDP application services on all traffic that you want to inspect.

SRX Series Services Gateways can be deployed in inline tap mode and sniffer mode (only high-end SRX Series devices). The sniffer mode is not supported on branch SRX Series devices.

Sniffer mode is supported only on the high-end SRX Series devices. You can use the sniffer mode of IDP deployment by configuring the interfaces in promiscuous mode and manipulating the traffic and flow setup with routing.

On all high-end SRX Series devices, in sniffer mode, ingress and egress interfaces work with flow showing both source and destination interface as egress interface.

As a workaround, in sniffer mode, use the tagged interfaces. Hence, the same interface names are displayed in the logs. For example, the ge-0/0/2.0 as ingress (sniff) and the ge-0/0/2.100 as egress interfaces are displayed in the logs to show the source interface as ge-0/0/2.100.

```
set interfaces ge-0/0/2 promiscuous-mode
set interfaces ge-0/0/2 vlan-tagging
set interfaces ge-0/0/2 unit 0 vlan-id 0
set interfaces ge-0/0/2 unit 100 vlan-id 100
```

**Related
Documentation**

- [Updating Licenses for a Branch SRX Series on page 35](#)
- [Example: Configuring Intrusion Detection and Prevention for SRX Series on page 50](#)

Example: Configuring Intrusion Detection and Prevention for SRX Series

For transit traffic to pass through IDP inspection, you configure a security policy and enable IDP application services on all traffic that you want to inspect.

This example shows how to configure a security policy to enable IDP services for the first time on traffic flowing on the device.

- [Requirements on page 50](#)
- [Overview on page 51](#)
- [Configuration on page 51](#)
- [Verification on page 54](#)

Requirements

Before you begin, install or verify an intrusion detection and prevention (IDP) feature license. See [“Updating Licenses for a Branch SRX Series” on page 35](#).

This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

Overview

In this example, you configure a policy to enable IDP services on an SRX210 to inspect all traffic from the untrust zone to the DMZ zone against the IDP rulebases.

As a first step, you must download and install the signature database from the Juniper Networks website. Next, download and install the predefined IDP policy templates and activate the predefined policy Recommended as the active policy.

Next, you must create a security policy from the untrust zone to DMZ zone and specify actions to be taken on the traffic that matches the conditions specified in the policy.

Configuration

Downloading and Installing the Signature Database

CLI Quick Configuration

CLI quick configuration is not available for this example because manual intervention is required during the configuration.

Step-by-Step Procedure

To configure an IDP policy:

1. Download the signature database.

[edit]

```
user@host# run request security idp security-package download
```

Will be processed in async mode. Check the status using the status checking CLI



NOTE: Downloading the database might take some time depending on the database size and the speed of your Internet connection.

2. Check the security package download status.

[edit]

```
user@host# run request security idp security-package download status
```

```
Done;Successfully downloaded
from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2230(Mon Feb 4 19:40:13 2013 GMT-8, Detector=12.6.160121210)
```

3. Install the attack database.

[edit]

```
user@host# run request security idp security-package install
```

Will be processed in async mode. Check the status using the status checking CLI



NOTE: Installing the attack database might take some time depending on the security database size.

4. Check the attack database install status. The command output displays information about the downloaded and installed versions of the attack database.

[edit]

user@host# run request security idp security-package install status

```
Done;Attack DB update : successful - [UpdateNumber=2230,ExportDate=Mon Feb
 4 19:40:13 2013 GMT-8,Detector=12.6.160121210]
Updating control-plane with new detector : successful
Updating data-plane with new attack or detector : successful
```

5. Confirm your IDP security package version.

[edit]

user@host# run show security idp security-package-version

```
Attack database version:2230(Mon Feb  4 19:40:13 2013 GMT-8)
Detector version :12.6.160121210
Policy template version :2230
```

6. Download the predefined IDP policy templates.

[edit]

user@host# run request security idp security-package download policy-templates

```
Will be processed in async mode. Check the status using the status checking
CLI
```

7. Check the security package download status.

[edit]

user@host# run request security idp security-package download status

```
Done;Successfully downloaded
from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2248
```

8. Install the IDP policy templates.

[edit]

user@host# run request security idp security-package install policy-templates

```
Will be processed in async mode. Check the status using the status checking
CLI
```

9. Verify the installation status update.

[edit]

user@host# run request security idp security-package install status

```
Done;policy-templates has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```

10. Enable the **templates.xsl** scripts file. On commit, the Junos OS management process (mgd) looks in to **templates.xsl** and installs the required policy.

[edit]

user@host# set system scripts commit file templates.xsl

11. Commit the configuration. The downloaded templates are saved to the Junos OS configuration database, and they are available in the CLI at the **[edit security idp idp-policy]** hierarchy level.

[edit]

user@host# commit

12. Display the list of downloaded templates.

```
[edit]
user@host# set security idp active-policy ?
```

```
Possible completions:
(active-policy)      Set active policy
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Web_Server
idp-engine
```

13. Activate the predefined Recommended policy as the active policy.

```
[edit]
user@host# set security idp active-policy Recommended
```

14. Confirm the active policy enabled on your device.

```
[edit]
user@host>show security idp active-policy
```

```
active-policy Recommended;
```

15. Create a security policy for the traffic from the untrust zone to the DMZ zone. In this step, you are creating an address set in the DMZ zone to group all HTTP server addresses together. In this example, you are applying security policies that can be used to inspect the traffic between the untrust zone and the DMZ zone.



NOTE: Keep in mind the following points:

- Security policy on order on SRX Series device is important because Junos OS performs a policy lookup starting from the top of the list, and when the device finds a match for the traffic received, it stops policy lookup.
- The SRX Series device allows you to enable IDP processing on a security policy on a rule-by-rule basis, instead of turning on IDP inspection across the device.
- A security policy identifies what traffic is to be sent to the IDP engine, and then the IDP engine applies inspection based on the contents of that traffic. Traffic that matches a security policy in which IDP is not enabled completely bypasses IDP processing. Traffic that matches a security policy marked for IDP processing is handed off to the IDP engine.

```
[edit]
user@host# set security zones security-zone DMZ address-book address
Server-HTTP-1 192.168.2.2/24
user@host# set security zones security-zone DMZ address-book address
Server-HTTP-2 192.168.2.3/24
```

```
user@host# set security zones security-zone DMZ address-book address-set
DMZ-address-set-http address Server-HTTP-1
user@host# set security zones security-zone DMZ address-book address-set
DMZ-address-set-http address Server-HTTP-2
user@host# set security policies from-zone untrust to-zone DMZ policy P1 match
source-address any
user@host# set security policies from-zone untrust to-zone DMZ policy P1 match
destination-address DMZ-address-set-http
user@host# set security policies from-zone untrust to-zone DMZ policy P1 match
application junos-http
```

16. Specify the action to be taken on traffic that matches conditions specified in the security policy. The security policy action must be to permit the flow.

```
[edit]
user@host# set security policies from-zone untrust to-zone DMZ policy P1 then
permit application-services idp
```

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

```
[edit]
user@srx210-host# show security policies
from-zone untrust to-zone DMZ {
  policy idp-app-policy-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          idp;
        }
      }
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

Verifying the IDP Configuration

Purpose Verify that the IDP configuration is working properly.

Action From operational mode, enter the **show security idp status** command.

```

user@srx210-host>show security idp status detail

PIC : FPC 0 PIC 0:
State of IDP: Default, Up since: 2013-01-22 02:51:15 GMT-8 (2w0d 20:30 ago)

Packets/second: 0           Peak: 0 @ 2013-02-05 23:06:20 GMT-8
KBits/second : 0           Peak: 0 @ 2013-02-05 23:06:20 GMT-8
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
[ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
ICMP: [Current: 0] [Max: 0 @ 2013-02-05 23:06:20 GMT-8]
TCP: [Current: 0] [Max: 0 @ 2013-02-05 23:06:20 GMT-8]
UDP: [Current: 0] [Max: 0 @ 2013-02-05 23:06:20 GMT-8]
Other: [Current: 0] [Max: 0 @ 2013-02-05 23:06:20 GMT-8]

Session Statistics:
[ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

```

ID	Name	Sessions	Memory	Detector
0	Recommended	0	2233	12.6.160121210

Meaning The sample output shows the Recommended predefined IDP policy as the active policy.

Related Documentation

- [Updating Licenses for a Branch SRX Series on page 35](#)
- [Understanding Intrusion Detection and Prevention for SRX Series on page 49](#)

Understanding Stateful Firewall, IPsec VPN, and Chassis Cluster for Branch SRX Series

- [Understanding Branch SRX Series Stateful Firewall Functionality on page 55](#)
- [Understanding IPsec VPN for SRX Series on page 56](#)
- [Understanding Chassis Cluster for SRX Series on page 56](#)

Understanding Branch SRX Series Stateful Firewall Functionality

Your branch SRX Series includes a stateful firewall, which tracks the state of each traffic flow or stream and uses dynamic packet inspection to identify patterns in data packets that might represent a threat to your network. This feature protects hosts from communicating with compromised or malicious users or applications.

The branch SRX Series uses zones and policies to provide firewall configuration.

Although zones and policies can have user-defined configurations, the factory-default configuration contains, at a minimum, a “trust” and “untrust” zone. The trust zone is used for configuration and attaching the internal LAN to the branch SRX Series. The untrust zone is commonly used for the WAN or untrusted Internet interface.

To simplify installation and make configuration easier, a default policy is in place that allows traffic originating from the trust zone to the untrust zone. You are not required to configure a deny policy from the untrust zone to any other zones, because the device drops the traffic by default if there is no policy defined for any traffic.

By using the J-Web interface or CLI, you can create a series of security policies that can control the traffic from within and in between zones by defining policies.

- Related Documentation**
- [Understanding Security Zones and Policies for SRX Series on page 23](#)
 - [Example: Configuring Security Zones and Policies for SRX Series on page 24](#)

Understanding IPsec VPN for SRX Series

A virtual private network (VPN) provides a means for securely communicating between remote computers across a public wide area network (WAN), such as the Internet. A VPN connection can link two local area networks (LAN) or a remote dialup user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN.

To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPsec) tunnel.

IPsec is a suite of protocols designed to authenticate and encrypt all IP traffic between two locations. IPsec allows trusted data to pass through networks that would otherwise be considered insecure. An IPsec tunnel consists of a pair of unidirectional Security Associations (SA); one at each end of the tunnel that specify the security parameter index (SPI), destination IP address, and security protocol (Authentication Header or Encapsulating Security Payload) employed.

Through the SA, an IPsec tunnel can provide the following security functions:

- Privacy (through encryption)
- Content integrity (through data authentication)
- Sender authentication

- Related Documentation**
- [VPN Feature Guide for Security Devices](#)

Understanding Chassis Cluster for SRX Series

Chassis clustering provides network node redundancy by grouping a pair of the same kind of supported SRX Series into a cluster. The devices must be running Junos OS. To form a chassis cluster, a pair of the same kind of supported SRX Series are combined to act as a single system that enforces the same overall security. The two nodes back each other up, with one node acting as the primary node and the other as the secondary node; this ensures stateful failover of processes and services in the event of system or hardware failure.

- Related Documentation**
- [Chassis Cluster Feature Guide for Security Devices](#)

CHAPTER 4

Configuration Statements and Operational Commands

- [Configuration Statements on page 57](#)
- [Operational Commands on page 88](#)

Configuration Statements

- [Security Configuration Statement Hierarchy on page 57](#)
- [\[edit security address-book\] Hierarchy Level on page 58](#)
- [\[edit security idp\] Hierarchy Level on page 59](#)
- [\[edit security ike\] Hierarchy Level on page 69](#)
- [\[edit security ipsec\] Hierarchy Level on page 70](#)
- [\[edit security nat\] Hierarchy Level on page 72](#)
- [\[edit security policies\] Hierarchy Level on page 75](#)
- [\[edit security utm\] Hierarchy Level on page 80](#)
- [\[edit security zones\] Hierarchy Level on page 87](#)

Security Configuration Statement Hierarchy

Use the statements in the **security** configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones. Statements that are exclusive to the SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the **[edit security]** hierarchy.

- [\[edit security address-book\] Hierarchy Level on page 58](#)
- [\[edit security alarms\] Hierarchy Level on page 1555](#)
- [\[edit security alg\] Hierarchy Level](#)

- [\[edit security analysis\] Hierarchy Level](#)
- [\[edit security application-firewall\] Hierarchy Level](#)
- [\[edit security application-tracking\] Hierarchy Level](#)
- [\[edit security certificates\] Hierarchy Level on page 1012](#)
- [\[edit security datapath-debug\] Hierarchy Level on page 1556](#)
- [\[edit security dynamic-vpn\] Hierarchy Level](#)
- [\[edit security firewall-authentication\] Hierarchy Level](#)
- [\[edit security flow\] Hierarchy Level](#)
- [\[edit security forwarding-options\] Hierarchy Level](#)
- [\[edit security forwarding-process\] Hierarchy Level](#)
- [\[edit security gprs\] Hierarchy Level](#)
- [\[edit security group-vpn\] Hierarchy Level](#)
- [\[edit security idp\] Hierarchy Level on page 59](#)
- [\[edit security ike\] Hierarchy Level on page 69](#)
- [\[edit security ipsec\] Hierarchy Level on page 70](#)
- [\[edit security log\] Hierarchy Level](#)
- [\[edit security nat\] Hierarchy Level on page 72](#)
- [\[edit security pki\] Hierarchy Level](#)
- [\[edit security policies\] Hierarchy Level on page 75](#)
- [\[edit security resource-manager\] Hierarchy Level](#)
- [\[edit security screen\] Hierarchy Level](#)
- [\[edit security softwires\] Hierarchy Level](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 1012](#)
- [\[edit security traceoptions\] Hierarchy Level on page 1557](#)
- [\[edit security user-identification\] Hierarchy Level](#)
- [\[edit security utm\] Hierarchy Level on page 80](#)
- [\[edit security zones\] Hierarchy Level on page 87](#)

Related Documentation

- [CLI User Guide](#)

[\[edit security address-book\] Hierarchy Level](#)

```
security {  
  address-book (book-name | global) {  
    address address-name {  
      ip-prefix {
```



```

        description text;
    }
    description text;
    dns-name domain-name {
        ipv4-only;
        ipv6-only;
    }
    range-address lower-limit to upper-limit;
    wildcard-address ipv4-address/wildcard-mask;
}
address-set address-set-name {
    address address-name;
    address-set address-set-name;
    description text;
}
attach {
    zone zone-name;
}
description text;
}
}

```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [Understanding Address Books](#)

[edit security idp] Hierarchy Level

```

security {
    idp {
        active-policy policy-name;
        custom-attack attack-name {
            attack-type {
                anomaly {
                    direction (any | client-to-server | server-to-client);
                    service service-name;
                    shellcode (all | intel | no-shellcode | sparc);
                    test test-condition;
                }
            }
            chain {
                expression boolean-expression;
                member member-name {
                    attack-type {
                        (anomaly ...same statements as in [edit security idp custom-attack
                        attack-name attack-type anomaly] hierarchy level | signature ...same
                        statements as in [edit security idp custom-attack attack-name attack-type
                        signature] hierarchy level);
                    }
                }
            }
            order;
            protocol-binding {
                application application-name;
                icmp;
                icmpv6;
                ip {

```

```
    protocol-number transport-layer-protocol-number;  
  }  
  ipv6 {  
    protocol-number transport-layer-protocol-number;  
  }  
  rpc {  
    program-number rpc-program-number;  
  }  
  tcp {  
    minimum-port port-number <maximum-port port-number>;  
  }  
  udp {  
    minimum-port port-number <maximum-port port-number>;  
  }  
}  
reset;  
scope (session | transaction);  
}  
signature {  
  context context-name;  
  direction (any | client-to-server | server-to-client);  
  negate;  
  pattern signature-pattern;  
  protocol {  
    icmp {  
      checksum-validate {  
        match (equal | greater-than | less-than | not-equal);  
        value checksum-value;  
      }  
      code {  
        match (equal | greater-than | less-than | not-equal);  
        value code-value;  
      }  
      data-length {  
        match (equal | greater-than | less-than | not-equal);  
        value data-length;  
      }  
      identification {  
        match (equal | greater-than | less-than | not-equal);  
        value identification-value;  
      }  
      sequence-number {  
        match (equal | greater-than | less-than | not-equal);  
        value sequence-number;  
      }  
      type {  
        match (equal | greater-than | less-than | not-equal);  
        value type-value;  
      }  
    }  
  }  
  icmpv6 {  
    checksum-validate {  
      match (equal | greater-than | less-than | not-equal);  
      value checksum-value;  
    }  
    code {
```

```

        match (equal | greater-than | less-than | not-equal);
        value code-value;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    type {
        match (equal | greater-than | less-than | not-equal);
        value type-value;
    }
}
ipv4 {
    checksum-validate {
        match (equal | greater-than | less-than | not-equal);
        value checksum-value;
    }
    destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
    }
    ihl {
        match (equal | greater-than | less-than | not-equal);
        value ihl-value;
    }
    ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
    }
    protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);

```

```
    value total-length-of-ip-datagram;
  }
  ttl {
    match (equal | greater-than | less-than | not-equal);
    value time-to-live;
  }
}
ipv6 {
  destination {
    match (equal | greater-than | less-than | not-equal);
    value ip-address-or-hostname;
  }
  extension-header {
    destination-option {
      home-address {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
      }
      option-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
      }
    }
    routing-header {
      header-type {
        match (equal | greater-than | less-than | not-equal);
        value header-value;
      }
    }
  }
}
flow-label {
  match (equal | greater-than | less-than | not-equal);
  value flow-label-value;
}
hop-limit {
  match (equal | greater-than | less-than | not-equal);
  value hop-limit-value;
}
next-header {
  match (equal | greater-than | less-than | not-equal);
  value next-header-value;
}
payload-length {
  match (equal | greater-than | less-than | not-equal);
  value payload-length-value;
}
source {
  match (equal | greater-than | less-than | not-equal);
  value ip-address-or-hostname;
}
traffic-class {
  match (equal | greater-than | less-than | not-equal);
  value traffic-class-value;
}
tcp {
  ack-number {
```

```
    match (equal | greater-than | less-than | not-equal);
    value acknowledgement-number;
}
checksum-validate {
    match (equal | greater-than | less-than | not-equal);
    value checksum-value;
}
data-length {
    match (equal | greater-than | less-than | not-equal);
    value tcp-data-length;
}
destination-port {
    match (equal | greater-than | less-than | not-equal);
    value destination-port;
}
header-length {
    match (equal | greater-than | less-than | not-equal);
    value header-length;
}
mss {
    match (equal | greater-than | less-than | not-equal);
    value maximum-segment-size;
}
option {
    match (equal | greater-than | less-than | not-equal);
    value tcp-option;
}
reserved {
    match (equal | greater-than | less-than | not-equal);
    value reserved-value;
}
sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number;
}
source-port {
    match (equal | greater-than | less-than | not-equal);
    value source-port;
}
tcp-flags {
    (ack | no-ack);
    (fin | no-fin);
    (psh | no-psh);
    (r1 | no-r1);
    (r2 | no-r2);
    (rst | no-rst);
    (syn | no-syn);
    (urg | no-urg);
}
urgent-pointer {
    match (equal | greater-than | less-than | not-equal);
    value urgent-pointer;
}
window-scale {
    match (equal | greater-than | less-than | not-equal);
    value window-scale-factor;
```

```

    }
    window-size {
        match (equal | greater-than | less-than | not-equal);
        value window-size;
    }
}
udp {
    checksum-validate {
        match (equal | greater-than | less-than | not-equal);
        value checksum-value;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
    }
}
}
protocol-binding {
    application application-name;
    icmp;
    icmpv6;
    ip {
        protocol-number transport-layer-protocol-number;
    }
    ipv6 {
        protocol-number transport-layer-protocol-number;
    }
    rpc {
        program-number rpc-program-number;
    }
    tcp {
        minimum-port port-number <maximum-port port-number>;
    }
    udp {
        minimum-port port-number <maximum-port port-number>;
    }
}
regexp regular-expression;
shellcode (all | intel | no-shellcode | sparc);
}
}
recommended-action (close | close-client | close-server | drop | drop-packet | ignore
| none);
severity (critical | info | major | minor | warning);
time-binding {
    count count-value;
    scope (destination | peer | source);
}
}

```

```

}
custom-attack-group custom-attack-group-name {
    group-members [attack-or-attack-group-name];
}
dynamic-attack-group dynamic-attack-group-name {
    filters {
        category {
            values [category-value];
        }
        direction {
            expression (and | or);
            values [any client-to-server exclude-any exclude-client-to-server
                exclude-server-to-client server-to-client];
        }
        false-positives {
            values [frequently occasionally rarely unknown];
        }
        performance {
            values [fast normal slow unknown];
        }
        products {
            values [product-value];
        }
        recommended;
        no-recommended;
        service {
            values [service-value];
        }
        severity {
            values [critical info major minor warning];
        }
        type {
            values [anomaly signature];
        }
    }
}
idp-policy policy-name {
    rulebase-exempt {
        rule rule-name {
            description text;
            match {
                attacks {
                    custom-attack-groups [attack-group-name];
                    custom-attacks [attack-name];
                    dynamic-attack-groups [attack-group-name];
                    predefined-attack-groups [attack-group-name];
                    predefined-attacks [attack-name];
                }
                destination-address ([address-name] | any | any-ipv4 | any-ipv6);
                destination-except [address-name];
                from-zone (zone-name | any );
                source-address ([address-name] | any | any-ipv4 | any-ipv6);
                source-except [address-name];
                to-zone (zone-name | any);
            }
        }
    }
}

```

```

}
rulebase-ips {
  rule rule-name {
    description text;
    match {
      application (application-name | any | default);
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
    terminal;
    then {
      action {
        class-of-service {
          dscp-code-point number;
          forwarding-class forwarding-class;
        }
        (close-client | close-client-and-server | close-server | drop-connection |
          drop-packet | ignore-connection | mark-diffserv value | no-action |
          recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        log-create;
        refresh-timeout;
        target (destination-address | service | source-address | source-zone |
          source-zone-address | zone-service);
        timeout seconds;
      }
      notification {
        log-attacks {
          alert;
        }
        packet-log {
          post-attack number;
          post-attack-timeout seconds;
          pre-attack number;
        }
      }
      severity (critical | info | major | minor | warning);
    }
  }
}
}
security-package {

```



```

automatic {
    download-timeout minutes;
    enable;
    interval hours;
    start-time start-time;
}
install {
    ignore-version-check;
}
source-address address;
url url-name;
}
sensor-configuration {
    application-identification {
        max-packet-memory-ratio percentage-value;
        max-reass-packet-memory-ratio percentage-value;
        max-tcp-session-packet-memory value;
        max-udp-session-packet-memory value;
    }
    detector {
        protocol-name protocol-name {
            tunable-name tunable-name {
                tunable-value protocol-value;
            }
        }
    }
}
flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    drop-if-no-policy-loaded;
    drop-on-failover;
    drop-on-limit;
    fifo-max-size value;
    hash-table-size value;
    (log-errors | no-log-errors);
    max-sessions-offset value;
    max-timers-poll-ticks value;
    min-objcache-limit-lt lower-threshold-value;
    min-objcache-limit-ut upper-threshold-value;
    reject-timeout value;
    (reset-on-policy | no-reset-on-policy);
    udp-anticipated-timeout value;
}
global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    gtp (decapsulation | no-decapsulation);
    memory-limit-percent value;
    (policy-lookup-cache | no-policy-lookup-cache);
}
high-availability {
    no-policy-cold-synchronization;
}
disable-low-memory-handling;
ips {
    content-decompression-max-memory-kb value;
    content-decompression-max-ratio value;
}

```

```

    (detect-shellcode | no-detect-shellcode);
    fifo-max-size value;
    (ignore-regular-expression | no-ignore-regular-expression);
    log-supercede-min minimum-value;
    pre-filter-shellcode;
    (process-ignore-s2c | no-process-ignore-s2c);
    (process-override | no-process-override);
    process-port port-number;
}
log {
    cache-size size;
    suppression {
        disable;
        (include-destination-address | no-include-destination-address);
        max-logs-operate value;
        max-time-report value;
        start-log value;
    }
}
packet-log {
    host ip-address <port number>;
    max-sessions percentage;
    source-address ip-address;
    total-memory percentage;
}
re-assembler {
    action-on-reassembly-failure (drop | drop-session | ignore);
    (force-tcp-window-checks | no-force-tcp-window-checks);
    (ignore-memory-overflow | no-ignore-memory-overflow);
    (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
    ignore-reassembly-overflow;
    max-flow-mem value;
    max-packet-mem-ratio percentnage-value;
    max-synacks-queued value;
    (tcp-error-logging | no-tcp-error-logging);
}
ssl-inspection {
    cache-prune-chunk-size number;
    key-protection;
    maximum-cache-size number;
    session-id-cache-timeout seconds;
    sessions number;
}
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag all;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}

```

```

    }
  }

```

Related Documentation

- [Security Configuration Statement Hierarchy on page 57](#)
- [Understanding Intrusion Detection and Prevention for SRX Series on page 49](#)

[edit security ike] Hierarchy Level

```

security {
  ike {
    gateway gateway-name {
      address [ip-address-or-hostname];
      dead-peer-detection {
        (always-send | optimized | probe-idle-tunnel);
        interval seconds;
        threshold number;
      }
    }
    dynamic {
      connections-limit number;
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
        e-mail-address);
      ike-user-type (group-ike-id | shared-ike-id);
    }
    external-interface external-interface-name;
    general-ikeid;
    ike-policy policy-name;
    local-address (ipv4-address | ipv6-address);
    local-identity {
      (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address
        | user-at-hostname e-mail-address);
    }
    nat-keepalive seconds;
    no-nat-traversal;
    remote-identity {
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
        e-mail-address);
    }
    version (v1-only | v2-only);
    xauth {
      access-profile profile-name;
    }
  }
  policy policy-name {
    certificate {
      local-certificate certificate-id;
      peer-certificate-type (pkcs7 | x509-signature);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard } suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
  }
}

```

```

}
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha-384 | sha1);
  authentication-method (dsa-signatures | ecdsa-signatures-256 |
    ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  lifetime-seconds seconds;
}
respond-bad-spi <max-responses>;
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    (no-world-readable | world-readable);
    size maximum-file-size;
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
}
}

```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [IPsec VPN Overview](#)

[edit security ipsec] Hierarchy Level

```

security {
  ipsec {
    internal {
      security-association {
        manual encryption {
          ikev2_encryption enabled;
          algorithm 3des-cbc;
          key ascii-text key;
        }
      }
    }
  }
  policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24
      | group5);
    proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96
      | hmac-sha1-96);
    description description;
  }
}

```

```

    encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc |
        aes-192-gcm | aes-256-cbc | aes-256-gcm | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
}
security-association sa-name {
    manual {
        direction bidirectional {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key {
                    ascii-text key;
                    hexadecimal key;
                }
            }
            auxiliary-spi auxiliary-spi-value;
            encryption {
                algorithm (3des-cbc | des-cbc | null);
                key {
                    ascii-text key;
                    hexadecimal key;
                }
            }
            protocol (ah | esp);
            spi spi-value;
        }
    }
    mode transport;
}
traceoptions {
    flag flag;
}
vpn vpn-name {
    bind-interface interface-name;
    df-bit (clear | copy | set);
    establish-tunnels (immediately | on-traffic);
    ike {
        gateway gateway-name;
        idle-time seconds;
        install-interval seconds;
        ipsec-policy ipsec-policy-name;
        no-anti-replay;
        proxy-identity {
            local ip-prefix;
            remote ip-prefix;
            service (any | service-name);
        }
    }
}
manual {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    }
}

```

```

        key (ascii-text key | hexadecimal key);
    }
    external-interface external-interface-name;
    gateway ip-address;
    protocol (ah | esp);
    spi spi-value;
}
traffic-selector traffic-selector-name {
    local-ip ip-address/netmask;
    remote-ip ip-address/netmask;
}
vpn-monitor {
    destination-ip ip-address;
    optimized;
    source-interface interface-name;
}
}
vpn-monitor-options {
    interval seconds;
    threshold number;
}
}
}

```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [IPsec VPN Overview](#)
 - [Understanding Logical Systems for SRX Series Services Gateways](#)

[edit security nat] Hierarchy Level

```

security {
  nat {
    destination {
      pool pool-name {
        address <ip-address> {
          (port port-number | to ip-address);
        }
        description text;
        routing-instance (routing-instance-name | default);
      }
      rule-set rule-set-name {
        description text;
        from {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
        rule rule-name {
          description text;
          match {
            application {
              [application];
              any;
            }
          }
        }
      }
    }
  }
}

```

```

        (destination-address ip-address | destination-address-name address-name);
        destination-port (port-or-low <to high>);
        protocol [protocol-name-or-number];
        source-address [ip-address];
        source-address-name [address-name];
    }
    then {
        destination-nat (off | pool pool-name | rule-session-count-alarm
            (clear-threshold value | raise-threshold value));
    }
}
}
}
}
proxy-arp interface interface-name address ip-address;
    to ip-address;
}
proxy-ndp interface interface-name address ip-address;
    to ip-address;
}
source {
    address-persistent;
    interface (port-overloading off | port-overloading-factor number);
    pool pool-name {
        address ip-address {
            to ip-address;
        }
        address-persistent subscriber ipv6-prefix-length prefix-length;
        address-pooling (paired | no-paired);
        address-shared;
        description text;
        host-address-base ip-address;
        overflow-pool (pool-name | interface);
        pool-utilization-alarm (clear-threshold value | raise-threshold value);
        port {
            block-allocation {
                active-block-timeout timeout-interval;
                block-size block-size;
                log disable;
                maximum-blocks-per-host maximum-block-number
            }
            deterministic {
                block-size block-size;
                host {
                    address ip-address;
                    address-name address-name;
                }
            }
            no-translation;
            port-overloading-factor number;
            range {
                port-low <to port-high>;
                to port-high;
                twin-port port-low <to port-high>;
            }
        }
    }
    routing-instance routing-instance-name;
}

```

```

pool-default-port-range lower-port-range to upper-port-range;
pool-default-twin-port-range lower-port-range to upper-port-range;
pool-utilization-alarm (clear-threshold value | raise-threshold value);
port-randomization disable;
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      application {
        [application];
        any;
      }
      (destination-address <ip-address> | destination-address-name
        <address-name>);
      destination-port (port-or-low <to high>);
      protocol [protocol-name-or-number];
      source-address [ip-address];
      source-address-name [address-name];
      source-port (port-or-low <to high>);
    }
    then source-nat;
    interface {
      persistent-nat {
        address-mapping;
        inactivity-timeout seconds;
        max-session-number value;
        permit (any-remote-host | target-host | target-host-port);
      }
    }
    off;
    pool <pool-name>
    persistent-nat
      address-mapping;
      inactivity-timeout seconds;
      max-session-number number;
      permit (any-remote-host | target-host | target-host-port);
  }
  rule-session-count-alarm (clear-threshold value | raise-threshold value);
}
}
to {
  interface [interface-name];
  routing-instance [routing-instance-name];
  zone [zone-name];
}
}
}
static rule-set rule-set-name;
description text;
from {
  interface [interface-name];

```



```

routing-instance [routing-instance-name];
zone [zone-name];
}
rule rule-name {
    description text;
    match {
        (destination-address <ip-address> | destination-address-name
         <address-name>);
        destination-port (port-or-low | <to high>);
        source-address [ip-address];
        source-address-name [address-name];
        source-port (port-or-low <to high>);
    }
    then static-nat;
    inet {
        routing-instance (routing-instance-name | default);
    }
    prefix {
        address-prefix;
        mapped-port lower-port-range to upper-port-range;
        routing-instance (routing-instance-name| default);
    }
    prefix-name {
        address-prefix-name;
        mapped-port lower-port-range to upper-port-range;
        routing-instance (routing-instance-name | default);
    }
    rule-session-count-alarm (clear-threshold value | raise-threshold value);
}
}
}
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (world-readable | no-world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
}

```

Related Documentation

- [Security Configuration Statement Hierarchy on page 57](#)
- *Understanding Logical Systems for SRX Series Services Gateways*
- *Introduction to NAT*

[edit security policies] Hierarchy Level

```
security {
```

```
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        destination-address-excluded;
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address-excluded;
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
      session-close;
      session-init;
    }
    permit {
      application-services {
        application-firewall {
          rule-set rule-set-name;
        }
      }
      application-traffic-control {
        rule-set rule-set-name;
      }
      gprs-gtp-profile profile-name;
      gprs-sctp-profile profile-name;
      idp;
    }
  }
}
```

```

    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
        profile-name profile-name;
    }
    uac-policy {
        captive-portal captive-portal;
    }
    utm-policy policy-name;
}
destination-address {
    drop-translated;
    drop-untranslated;
}
firewall-authentication {
    pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
    }
    user-firewall {
        access-profile profile-name;
        domain domain-name
        ssl-termination-profile profile-name;
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    sequence-check-required;
    syn-check-required;
}
tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
}
}
reject;
}
}
global {
    policy policy-name {
        description description;
        match {
            application {
                [application];
                any;
            }
            destination-address {
                [address];
                any;
            }
        }
    }
}

```

```
    any-ipv4;
    any-ipv6;
  }
  from-zone {
    [zone-name];
    any;
  }
  source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
  }
  source-identity {
    [role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
  }
  to-zone {
    [zone-name];
    any;
  }
}
scheduler-name scheduler-name;
then {
  count {
    alarm {
      per-minute-threshold number;
      per-second-threshold number;
    }
  }
  deny;
  log {
    session-close;
    session-init;
  }
  permit {
    application-services {
      application-firewall {
        rule-set rule-set-name;
      }
      application-traffic-control {
        rule-set rule-set-name;
      }
      gprs-gtp-profile profile-name;
      gprs-sctp-profile profile-name;
      idp;
      redirect-wx | reverse-redirect-wx;
      ssl-proxy {
        profile-name profile-name;
      }
      uac-policy {
        captive-portal captive-portal;
      }
    }
  }
}
```

```

        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            ssl-termination-profile profile-name;
            web-redirect;
            web-redirect-to-https;
        }
        user-firewall {
            access-profile profile-name;
            domain domain-name;
            ssl-termination-profile profile-name;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        initial-tcp-mss mss-value;
        reverse-tcp-mss mss-value;
        sequence-check-required;
        syn-check-required;
    }
    }
    reject;
}
}
}
policy-rematch;
policy-stats {
    system-wide (disable | enable);
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
}
}
}

```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [Understanding Security Building Blocks for Security Devices](#)

- *Unified Threat Management Overview*

[edit security utm] Hierarchy Level

```
security {
  utm {
    application-proxy {
      traceoptions {
        flag flag;
      }
    }
    custom-objects {
      custom-url-category object-name {
        value [value];
      }
      filename-extension object-name {
        value [value];
      }
      mime-pattern object-name {
        value [value];
      }
      protocol-command object-name {
        value [value];
      }
      url-pattern object-name {
        value [value];
      }
    }
  }
  feature-profile {
    anti-spam {
      address-blacklist list-name;
      address-whitelist list-name;
      sbl {
        profile profile-name {
          custom-tag-string [string];
          (sbl-default-server | no-sbl-default-server);
          spam-action (block | tag-header | tag-subject);
        }
      }
      traceoptions {
        flag flag;
      }
    }
    anti-virus {
      juniper-express-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
          proxy {
```

```

    password password-string;
    port port-number;
    server address-or-url;
    username name;
  }
  url url;
}
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
kaspersky-lab-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
  }
}

```

```
no-autoupdate;
proxy {
  password password-string;
  port port-number;
  server address-or-url;
  username name;
}
url url;
}
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    corrupt-file (block | log-and-permit);
    decompress-layer (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | log-and-permit);
    password-file (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
}
scan-options {
  content-size-limit value;
  decompress-layer-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  scan-extension filename;
  scan-mode (all | by-extension);
  timeout value;
}
trickling {
  timeout value;
}
}
```



```

mime-whitelist {
    exception listname;
    list listname {
        exception listname;
    }
}
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
    }
    scan-options {
        content-size-limit value;
    }
}

```

```
        (no-uri-check | uri-check);
        timeout value;
    }
    trickling {
        timeout value;
    }
}
sxl-retry value;
sxl-timeout seconds;
}
traceoptions {
    flag flag;
}
type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
url-whitelist listname;
}
content-filtering {
    profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
            exception list-name;
            list list-name;
        }
        notification-options {
            custom-message message;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
        }
        permit-command protocol-command-list;
    }
    traceoptions {
        flag flag;
    }
}
web-filtering {
    juniper-enhanced {
        cache {
            size value;
            timeout value;
        }
        profile profile-name {
            block-message {
                type {
                    custom-redirect-url;
                }
                url url;
            }
            quarantine-message {
                type {
                    custom-redirect-url;
                }
                url url;
            }
        }
        category customurl-list name {
```

```

    action (block | log-and-permit | permit | quarantine);
  }
  custom-block-message value;
  custom-quarantine-message value;
  default (block | log-and-permit | permit | quarantine);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  no-safe-search;
  site-reputation-action {
    fairly-safe (block | log-and-permit | permit | quarantine);
    harmful (block | log-and-permit | permit | quarantine);
    moderately-safe (block | log-and-permit | permit | quarantine);
    suspicious (block | log-and-permit | permit | quarantine);
    very-safe (block | log-and-permit | permit | quarantine);
  }
  timeout value;
}
server {
  host host-name;
  port number;
}
}
juniper-local {
  profile profile-name {
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    timeout value;
  }
}
surf-control-integrated {
  cache {
    size value;
    timeout value;
  }
  profile profile-name {
    category customurl-list name {
      action (block | log-and-permit | permit);
    }
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
  }
}

```

```
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
traceoptions {
    flag flag;
}
type (juniper-enhanced | juniper-local | surf-control-integrated |
    websense-redirect);
url-blacklist listname;
url-whitelist listname;
websense-redirect {
    profile profile-name {
        account value;
        custom-block-message value;
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        server {
            host host-name;
            port number;
        }
        sockets value;
        timeout value;
    }
}
}
}
ipc {
    traceoptions flag flag;
}
traceoptions {
    flag flag;
}
utm-policy policy-name {
    anti-spam {
        smtp-profile profile-name;
    }
    anti-virus {
        ftp {
            download-profile profile-name;
            upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
    }
    content-filtering {
        ftp {
```

```

        download-profile profile-name;
        upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
}
traffic-options {
    sessions-per-client {
        limit value;
        over-limit (block | log-and-permit);
    }
}
web-filtering {
    http-profile profile-name;
}
}
}
}
}

```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [Unified Threat Management Overview](#)

[\[edit security zones\]](#) Hierarchy Level

```

security {
    zones {
        functional-zone {
            management {
                description text;
                host-inbound-traffic {
                    protocols protocol-name {
                        except;
                    }
                    system-services service-name {
                        except;
                    }
                }
            }
            interfaces interface-name {
                host-inbound-traffic {
                    protocols protocol-name {
                        except;
                    }
                    system-services service-name {
                        except;
                    }
                }
            }
            screen screen-name;
        }
    }
    security-zone zone-name {
        address-book {

```

```
address address-name {
  ip-prefix {
    description text;
  }
  description text;
  dns-name domain-name {
    ipv4-only;
    ipv6-only;
  }
  range-address lower-limit to upper-limit;
  wildcard-address ipv4-address/wildcard-mask;
}
address-set address-set-name {
  address address-name;
  address-set address-set-name;
  description text;
}
}
application-tracking;
description text;
host-inbound-traffic {
  protocols protocol-name {
    except;
  }
  system-services service-name {
    except;
  }
}
}
interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
}
}
screen screen-name;
tcp-rst;
}
}
```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
 - [Understanding Logical Systems for SRX Series Services Gateways](#)
 - [Security Zones and Interfaces Overview](#)

Operational Commands

- [request system license update](#)
- [show security flow session](#)

- `show security idp active-policy`
- `show security idp status`
- `show security nat destination summary`
- `show security policies`
- `show security utm session`
- `show security utm status`
- `show security zones`
- `show system license (View)`
- `show system services dhcp client`

request system license update

Syntax	request system license update
Release Information	Command introduced in Junos OS Release 9.5.
Description	Start autoupdating license keys from the LMS server.
Options	trial —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 115
List of Sample Output	request system license update on page 90 request system license update trial on page 90
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.
```


show security flow session

Syntax	show security flow session [<i>filter</i>] [brief extensive summary]
Release Information	Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2. Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2. Policy ID filter added in Junos OS Release 12.3X48-D10.
Description	Display information about all currently active security sessions on the device.
Options	<ul style="list-style-type: none"> • <i>filter</i>—Filter the display by the specified criteria. The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific show command for examples of the filtered output. <p>application—Predefined application name</p> <p>application-firewall—Application firewall enabled</p> <p>application-firewall-rule-set—Application firewall enabled with the specified rule set</p> <p>application-traffic-control—Application traffic control session</p> <p>application-traffic-control-rule-set—Application traffic control rule set name and rule name</p> <p>destination-port—Destination port</p> <p>destination-prefix—Destination IP prefix or address</p> <p>dynamic-application—Dynamic application</p> <p>dynamic-application-group—Dynamic application</p> <p>encrypted—Encrypted traffic</p> <p>extensive—Display detailed output</p> <p>family—Display session by family</p> <p>idp—IDP enabled sessions</p> <p>interface—Name of incoming or outgoing interface</p> <p>logical-system (all <i>logical-system-name</i>)—Name of a specific logical system or all to display all logical systems</p> <p>nat—Display sessions with network address translation</p> <p>policy-id—Display session information based on policy ID; the range is 1 through 4,294,967,295</p>

protocol—IP protocol number

resource-manager—Resource manager

root-logical-system—Display root logical system as default

security-intelligence—Display security intelligence sessions

services-offload—Display services offload sessions

session-identifier—Display session with specified session identifier

source-port—Source port

source-prefix—Source IP prefix

summary—Display output summary

tunnel—Tunnel sessions

- **brief | extensive | summary**—Display the specified level of output.
- **none**—Display information about all active sessions.

Required Privilege Level view

Related Documentation

- *Juniper Networks Devices Processing Overview*
- *clear security flow session all*

List of Sample Output

[show security flow session on page 94](#)
[show security flow session brief on page 94](#)
[show security flow session extensive on page 95](#)
[show security flow session summary on page 95](#)

Output Fields [Table 12 on page 92](#) lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 12: show security flow session Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

Table 12: show security flow session Output Fields (*continued*)

Field Name	Field Description
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes. The three available flags are: <ul style="list-style-type: none"> • flag • natflag • natflag2
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Dynamic application	Name of the application.
Application traffic control rule-set	AppQoS rule set for this session.
Rule	AppQoS rule for this session.
Forwarding class	The AppQoS forwarding class name for this session that distinguishes the transmission priority
DSCP code point	Differentiated Services (DiffServ) code point (DSCP) value remarked by the matching rule for this session.
Loss priority	One of four priority levels set by the matching rule to control discarding a packet during periods of congestion. A high loss priority means a high probability that the packet could be dropped during a period of congestion.
Rate limiter client to server	The rate-limiter profile assigned to the client-to-server traffic defining a unique combination of bandwidth-limit and burst-size-limit specifications.
Rate limiter server to client	The rate-limiter profile assigned to the server-to-client traffic defining a unique combination of bandwidth-limit and burst-size-limit specifications.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.

Table 12: show security flow session Output Fields (*continued*)

Field Name	Field Description
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. <ul style="list-style-type: none"> Valid sessions Pending sessions Invalidated sessions Sessions in other states
Maximum-sessions	Maximum number of sessions permitted.

Sample Output

show security flow session

```

root> show security flow session
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0

```

show security flow session brief

```

root> show security flow session brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0

```

show security flow session extensive

```

root> show security flow session extensive
Flow Sessions on FPC5 PIC0:

Session ID: 100000001, Status: Normal
Flags: 0x8000052, 0x85a0000, 0x100,
Policy name: p/4
Source NAT pool: Null
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 296
Session State: Valid
Start time: 422, Duration: 4
  In: 15.0.0.10/3000 --> 20.0.0.10/3000;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x8, Flag: 0x21
    Route: 0x0, Gateway: 15.0.0.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 104
  Out: 20.0.0.10/3000 --> 15.0.0.10/3000;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x9, Flag: 0x20
    Route: 0x0, Gateway: 20.0.0.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

```

show security flow session summary

```

root> show security flow session summary
Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0

```

```
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Maximum-sessions: 819200
```

show security idp active-policy

Syntax	show security idp active-policy
Release Information	Command introduced in Junos OS Release 9.2.
Description	Display information about the policy name and running detector version with which the policy is compiled from the IDP data plane module.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>request security idp security-package download</i> <i>request security idp security-package install</i>
List of Sample Output	show security idp active-policy on page 97
Output Fields	<p>Table 13 on page 97 lists the output fields for the show security idp active-policy command. Output fields are listed in the approximate order in which they appear.</p>

Table 13: show security idp active-policy Output Fields

Field Name	Field Description
Policy Name	Name of the running policy.
Running Detector Version	Current version of the running detector.

Sample Output

show security idp active-policy

```

user@host> show security idp active-policy
Policy Name : viking-policy
Running Detector Version : 9.1.140080300

```

show security idp status

Syntax	show security idp status
Release Information	Command introduced in Junos OS Release 9.2. Multiple detector information introduced in Junos OS Release 10.1. Output changed to support IDP dedicated mode in Junos OS Release 11.2.
Description	Display the status of the current IDP policy.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Security Configuration Statement Hierarchy on page 57
List of Sample Output	show security idp status on page 99
Output Fields	Table 14 on page 98 lists the output fields for the show security idp status command. Output fields are listed in the approximate order in which they appear.

Table 14: show security idp status Output Fields

Field Name	Field Description
State of IDP	Status of current IDP policy.
Packets/second	The aggregated throughput (packets per second) for the system.
KBits/second	The aggregated throughput (kilobits per second) for the system.
Latency	<ul style="list-style-type: none"> • min—Minimum delay for a packet to receive and return by a node in microseconds. • max—Maximum delay for a packet to receive and return by a node in microseconds. • ave—Average delay for a packet to receive and return by a node in microseconds.
Packet Statistics	Statistics for ICMP, TCP, and UDP packets.
Flow Statistics	Flow-related system statistics for ICMP, TCP, and UDP packets.
Session Statistics	Session-related system statistics for ICMP, TCP, and UDP packets.
Number of SSL Sessions	Number of current SSL sessions.
Policy Name	Name of the running policy. If IDP is configured for logical systems, idp-policy-combined is displayed.
Running Detector Version	Current version of the running detector.
Forwarding process mode	IDP dedicated mode: default , equal , idp , or firewall .

Sample Output

show security idp status

```
user@host> show security idp status
State of IDP: 2-default, Up since: 2010-02-04 13:37:16 UTC (17:15:02 ago)

Packets/second: 5                Peak: 11 @ 2010-02-05 06:51:58 UTC
KBits/second   : 2                Peak: 5 @ 2010-02-05 06:52:06 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
[ICMP: 0] [TCP: 82] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  TCP:  [Current: 2] [Max: 6 @ 2010-02-05 06:52:08 UTC]
  UDP:  [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  Other: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]

Session Statistics:
[ICMP: 0] [TCP: 1] [UDP: 0] [Other: 0]

Policy Name : sample
Running Detector Version : 10.4.160091104
```

show security nat destination summary

Syntax	show security nat destination summary <logical-system (<i>logical-system-name</i> all)> <root-logical-system>
Release Information	Command introduced in Junos OS Release 9.2. Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10.
Description	Display a summary of Network Address Translation (NAT) destination pool information.
Options	<p>none—Display summary information about the destination NAT pool.</p> <p>logical-system (<i>logical-system-name</i> all)—Display summary information about the destination NAT for the specified logical system or for all logical systems.</p> <p>root-logical-system—Display summary information about the destination NAT for the master (root) logical system.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>pool (Security Destination NAT)</i> <i>rule (Security Destination NAT)</i> Security Configuration Statement Hierarchy on page 57
List of Sample Output	show security nat destination summary on page 101
Output Fields	Table 15 on page 100 lists the output fields for the show security nat destination summary command. Output fields are listed in the approximate order in which they appear.

Table 15: show security nat destination summary Output Fields

Field Name	Field Description
Total destination nat pool number	Number of destination NAT pools.
Pool name	Name of the destination address pool.
Address range	IP address or IP address range for the pool.
Routing Instance	Name of the routing instance.
Port	Port number.
Total	Number of IP addresses that are in use.
Available	Number of IP addresses that are free for use.
Total destination nat rule number	Number of destination NAT rules.

Table 15: show security nat destination summary Output Fields (*continued*)

Field Name	Field Description
Total hit times	Number of times a translation in the translation table is used for all the destination NAT rules.
Total fail times	Number of times a translation in the translation table failed to translate for all the destination NAT rules.

Sample Output

show security nat destination summary

```
user@host> show security nat destination summary
```

```

Total pools: 2
Pool name      Address Range      Routing Instance  Port  Total Address
dst-p1         1.1.1.1 - 1.1.1.1         default         0     1
dst-p2         2001::1 - 2001::1  default         0     1

Total rules: 171
Rule name      Rule set  From      Action
dst2-rule      dst2      ri1
               ri2
               ri3
               ri4
               ri5
               ri6
               ri7
dst3-rule      dst3      ri9
               ri1
               ri2
               ri3
               ri4
               ri5

...

```

show security policies

Syntax	<pre>show security policies <detail> <none> policy-name <i>policy-name</i> <detail> <global></pre>
Release Information	<p>Command modified in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations in addition to the existing support of active/passive chassis cluster configurations added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1. Support for global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The Description output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10. The output fields for Policy Statistics expanded, and the output fields for the global and policy-name options expanded to include from-zone and to-zone global match criteria in Junos OS Release 12.1X47-D10. Support for the initial-tcp-mss and reverse-tcp-mss options added in Junos OS Release 12.3X48-D20.</p>
Description	<p>Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.</p>
Options	<ul style="list-style-type: none"> • none—Display basic information about all configured policies. • detail—(Optional) Display a detailed view of all of the policies configured on the device. • policy-name <i>policy-name</i>—(Optional) Display information about the specified policy. • global—Display information about global policies.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Security Policies Overview</i> • <i>Understanding Security Policy Rules</i> • <i>Understanding Security Policy Elements</i> • <i>Building Blocks Feature Guide for Security Devices</i>
List of Sample Output	<p>show security policies on page 105 show security policies policy-name p1 detail on page 106 show security policies (services-offload) on page 107 show security policies detail on page 107 show security policies detail (TCP Options) on page 108 show security policies policy-name p1 (Negated Address) on page 108 show security policies policy-name p1 detail (Negated Address) on page 109 show security policies global on page 109</p>

Output Fields Table 16 on page 103 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Table 16: show security policies Output Fields

Field Name	Field Description
From zone	Name of the source zone.
To zone	Name of the destination zone.
Policy	Name of the applicable policy.
Description	Description of the applicable policy.
State	Status of the policy: <ul style="list-style-type: none"> • enabled: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. • disabled: The policy cannot be used in the policy lookup process, and therefore it is not available for access control.
Index	Internal number associated with the policy.
Sequence number	Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, 4.
Source addresses	For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.
Source addresses (excluded)	Name of the source address excluded from the policy.
Destination addresses (excluded)	Name of the destination address excluded from the policy.
Source identities	One or more user roles specified for a policy.

Table 16: show security policies Output Fields (*continued*)

Field Name	Field Description
Applications	<p>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</p> <ul style="list-style-type: none"> • IP protocol: The Internet protocol used by the application—for example, TCP, UDP, ICMP. • ALG: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If application-protocol ignore is configured, ignore is displayed. Otherwise, 0 is displayed. However, even if this command shows ALG: 0, ALGs might be triggered for packets destined to well-known ports on which ALGs are listening, unless ALGs are explicitly disabled or when application-protocol ignore is not configured for custom applications. • Inactivity timeout: Elapsed time without activity after which the application is terminated. • Source port range: The low-high source port range for the session application.
Destination Address Translation	<p>Status of the destination address translation traffic:</p> <ul style="list-style-type: none"> • drop translated—Drop the packets with translated destination addresses. • drop untranslated—Drop the packets without translated destination addresses.
Application Firewall	<p>An application firewall includes the following:</p> <ul style="list-style-type: none"> • Rule-set—Name of the rule set. • Rule—Name of the rule. <ul style="list-style-type: none"> • Dynamic applications—Name of the applications. • Dynamic application groups—Name of the application groups. • Action—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following: <ul style="list-style-type: none"> • permit • deny • Default rule—The default rule applied when the identified application is not specified in any rules of the rule set.
Action or Action-type	<ul style="list-style-type: none"> • The action taken in regard to a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> • permit • firewall-authentication • tunnel ipsec-vpn <i>vpn-name</i> • pair-policy <i>pair-policy-name</i> • source-nat pool <i>pool-name</i> • pool-set <i>pool-set-name</i> • interface • destination-nat <i>name</i> • deny • reject • services-offload
Session log	<p>Session log entry that indicates whether the at-create and at-close flags were set at configuration time to log session information.</p>

Table 16: show security policies Output Fields (*continued*)

Field Name	Field Description
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active and can be used as a possible match for traffic.
Policy statistics	<ul style="list-style-type: none"> • Input bytes—The total number of bytes presented for processing by the device. <ul style="list-style-type: none"> • Initial direction—The number of bytes presented for processing by the device from the initial direction. • Reply direction—The number of bytes presented for processing by the device from the reply direction. • Output bytes—The total number of bytes actually processed by the device. <ul style="list-style-type: none"> • Initial direction—The number of bytes from the initial direction actually processed by the device. • Reply direction—The number of bytes from the reply direction actually processed by the device. • Input packets—The total number of packets presented for processing by the device. <ul style="list-style-type: none"> • Initial direction—The number of packets presented for processing by the device from the initial direction. • Reply direction—The number of packets presented for processing by the device from the reply direction. • Output packets—The total number of packets actually processed by the device. <ul style="list-style-type: none"> • Initial direction—The number of packets actually processed by the device from the initial direction. • Reply direction—The number of packets actually processed by the device from the reply direction. • Session rate—The total number of active and deleted sessions. • Active sessions—The number of sessions currently present because of access control lookups that used this policy. • Session deletions—The number of sessions deleted since system startup. • Policy lookups—The number of times the policy was accessed to check for a match. <p>NOTE: Configure the Policy P1 with the count option to display policy statistics.</p>
Per policy TCP Options	Configured sync and sequence checks, and the configured TCP MSS value for the initial direction and /or the reverse direction.

Sample Output

show security policies

```

user@host> show security policies
From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Sequence number: 1
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
sa-4-wc: 192.168.0.11/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32

```

```

da-3-ipv6: 2400:0d78:0/24
da-4-wc: 192.168.22.11/255.255.0.255
Source identities: role1, role2, role4
Applications: any
Action: permit, application services, log, scheduled
Application firewall : my_ruleset1
Policy: p2, State: enabled, Index: 5, Sequence number: 2
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32
da-3-ipv6: 2400:0d78:0/24
Source identities: role1, role4
Applications: any
Action: deny, scheduled

```

show security policies policy-name p1 detail

```

user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
sa-1-ipv4: 2.2.2.0/24
sa-2-ipv6: 2001:0db8::/32
sa-3-ipv6: 2001:0db6/24
sa-4-wc: 192.168.0.11/255.255.0.255
Destination addresses:
da-1-ipv4: 2.2.2.0/24
da-2-ipv6: 2400:0af8::/32
da-3-ipv6: 2400:0d78:0/24
da-4-wc: 192.168.22.11/255.255.0.255
Source identities:
role1
role2
role4
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Destination Address Translation: drop translated
Application firewall :
Rule-set: my_ruleset1
Rule: rule1
Dynamic Applications: junos:FACEBOOK, junos:YSMG
Dynamic Application groups: junos:web, junos:chat
Action: deny
Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
Input bytes      : 18144      545 bps
Initial direction: 9072      272 bps
Reply direction  : 9072      272 bps
Output bytes     : 18144      545 bps
Initial direction: 9072      272 bps

```


Reply direction :	9072	272 bps
Input packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Output packets :	216	6 pps
Initial direction:	108	3 bps
Reply direction :	108	3 bps
Session rate :	108	3 sps
Active sessions :	93	
Session deletions :	15	
Policy lookups :	108	

show security policies (services-offload)

```

user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload

```

show security policies detail

```

user@host> show security policies detail
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
4, Scope Policy: 0
Policy Type: Configured
Description: The policy p1 is for the sales team
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Policy statistics:
  Input bytes      :      18144      545 bps
  Initial direction:      9072      272 bps
  Reply direction  :      9072      272 bps
  Output bytes     :      18144      545 bps

```

```

Initial direction:          9072          272 bps
Reply direction :          9072          272 bps
Input packets :            216           6 pps
Initial direction:          108           3 bps
Reply direction :          108           3 bps
Output packets :            216           6 pps
Initial direction:          108           3 bps
Reply direction :          108           3 bps
Session rate :             108           3 sps
Active sessions :           93
Session deletions :         15
Policy lookups :            108

Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
5, Scope Policy: 0
Policy Type: Configured
Description: The policy p2 is for the sales team
Sequence number: 1
From zone: untrust, To zone: trust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Source identities:
  role1
  role2
  role4
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

show security policies detail (TCP Options)

```

user@host> show security policies policy-name policy1 detail
node0:
-----
Policy: policy1, action-type: permit, State: enabled, Index: 7, Scope Policy: 0
Policy Type: Configured
Sequence number: 2
From zone: trust, To zone: untrust
Source addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Destination addresses:
  any-ipv4(global): 0.0.0.0/0
  any-ipv6(global): ::/0
Application: any
  IP protocol: 0, ALG: 0, Inactivity timeout: 0
  Source port range: [0-0]
  Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No
Per policy TCP MSS: initial: 800, reverse: 900

```

show security policies policy-name p1 (Negated Address)

```

user@host> show security policies policy-name p1
node0:
-----

```

```

From zone: trust, To zone: untrust
Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
Source addresses(excluded): as1
Destination addresses(excluded): as2
Applications: any
Action: permit

```

show security policies policy-name p1 detail (Negated Address)

```

user@host>show security policies policy-name p1 detail
node0:
-----
Policy: p1, action-type: permit, State: enabled, Index: 4, Scope Policy: 0
Policy Type: Configured
Sequence number: 1
From zone: trust, To zone: untrust
Source addresses(excluded):
  ad1(ad): 255.255.255.255/32
  ad2(ad): 1.1.1.1/32
  ad3(ad): 15.100.199.56 ~ 15.200.100.16
  ad4(ad): 15.100.196.0/22
  ad5(ad): 15.1.7.199 ~ 15.1.8.19
  ad6(ad): 15.1.8.0/21
  ad7(ad): 15.1.7.0/24
Destination addresses(excluded):
  ad13(ad2): 20.1.7.0/24
  ad12(ad2): 20.1.4.1/32
  ad11(ad2): 20.1.7.199 ~ 20.1.8.19
  ad10(ad2): 50.1.4.0/22
  ad9(ad2): 20.1.1.11 ~ 50.1.5.199
  ad8(ad2): 2.1.1.1/32
Application: any
IP protocol: 0, ALG: 0, Inactivity timeout: 0
Source port range: [0-0]
Destination port range: [0-0]
Per policy TCP Options: SYN check: No, SEQ check: No

```

show security policies global

```

user@host>show security policies global policy-name Pa
node0:
-----
Global policies:
Policy: Pa, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
From zones: zone1, zone2
To zones: zone3, zone4
Source addresses: any
Destination addresses: any
Applications: any
Action: permit

```

show security utm session

Syntax	show security utm session
Release Information	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
Description	Display general UTM session information including all allocated sessions and active sessions. Also, display information from both nodes in a chassis cluster.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>clear security utm session</i>• show security utm status on page 111
Output Fields	show security utm session Output fields are listed in the approximate order in which they appear.

show security utm session

```
user@host> show security utm session
Maximum sessions:      4000
Total allocated sessions: 0
Total freed sessions:  0
Active sessions:       0
```

show security utm status

Syntax	show security utm status
Release Information	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
Description	Display whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>clear security utm session</i>• show security utm session on page 110
Output Fields	show security utm status Output fields are listed in the approximate order in which they appear.

show security utm status

```
user@host> show security utm status
UTM service status: Running
```

show security zones

Syntax	show security zones <detail terse> < zone-name >
Release Information	Command introduced in Junos OS Release 8.5. The Description output field added in Junos OS Release 12.1.
Description	Display information about security zones.
Options	<ul style="list-style-type: none"> • none—Display information about all zones. • detail terse—(Optional) Display the specified level of output. • zone-name —(Optional) Display information about the specified zone.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Security Zones and Interfaces Overview</i> • <i>Supported System Services for Host Inbound Traffic</i> • <i>security-zone</i> • <i>Building Blocks Feature Guide for Security Devices</i>
List of Sample Output	show security zones on page 113 show security zones abc on page 113 show security zones abc detail on page 113 show security zones terse on page 114
Output Fields	Table 17 on page 112 lists the output fields for the show security zones command. Output fields are listed in the approximate order in which they appear.

Table 17: show security zones Output Fields

Field Name	Field Description
Security zone	Name of the security zone.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.
Zone	Name of the zone.

Table 17: show security zones Output Fields (*continued*)

Field Name	Field Description
Type	Type of the zone.

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

```

Sample Output

show security zones abc

```

user@host> show security zones abc
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

```

Sample Output

show security zones abc detail

```

user@host> show security zones abc detail
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
```

Sample Output

show security zones terse

```
user@host> show security zones terse
Zone           Type
my-internal    Security
my-external    Security
dmz            Security
```


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"> • Working with License Keys for SRX Series Devices on page 209
List of Sample Output	<p>show system license on page 116</p> <p>show system license installed on page 116</p> <p>show system license keys on page 117</p> <p>show system license usage on page 117</p> <p>show system license status logical-system all on page 117</p>
Output Fields	Table 18 on page 115 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 18: 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 18: 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	1	1	0	2012-03-30
01:00:00 IST				
wf_key_surfcontrol_cpa	0	1	0	2012-03-30
01:00:00 IST				
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 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.
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"> • dhcp (Interfaces) • request system services dhcp on page 1200
List of Sample Output	show system services dhcp client on page 119 show system services dhcp client ge-0/0/1.0 on page 119 show system services dhcp client statistics on page 120
Output Fields	Table 19 on page 118 lists the output fields for the show system services dhcp client command. Output fields are listed in the approximate order in which they appear.

Table 19: 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 at	Date and time the lease expires.
DHCP Options	<ul style="list-style-type: none"> • Name: <code>server-identifier</code>, Value: IP address of the name server. • Name: <code>device</code>, Value: IP address of the name device. • Name: <code>domain-name</code>, Value: Name of the domain.

Table 19: show system services dhcp client Output Fields (*continued*)

Field Name	Field Description
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-0/0/1.0
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
update server            enabled
Lease Obtained at        2006-08-24 18:13:04 PST
Lease Expires at         2006-08-25 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: domain-name, Value: netscreen-50

```

Sample Output

show system services dhcp client ge-0/0/1.0

```

user@host> show system services dhcp client ge-0/0/1.0

```

```
Logical Interface name      ge-0/0/1.0
Hardware address           00:12:1e:a9:7b:81
Client status              bound
Address obtained           30.1.1.20
Update server              disabled
Lease obtained at         2007-05-10 18:16:18 UTC
Lease expires at          2007-05-11 18:16:18 UTC
DHCP options:
  Name: server-identifier, Value: 30.1.1.2
  Code: 1, Type: ip-address, Value: 255.255.255.0
  Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
  Name: domain-name, Value: mylab.example.net
```

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
```

PART 2

Installation and Upgrade Guide for Security Devices

- [Junos Software and Hardware Overview on page 123](#)
- [Installing Junos OS Software on page 133](#)
- [Installing and Managing Software Licenses on page 195](#)
- [Configuration Statements and Operational Commands on page 217](#)

CHAPTER 5

Junos Software and Hardware Overview

- [Software Overview on page 123](#)
- [Hardware Overview on page 130](#)

Software Overview

- [Junos OS Overview on page 123](#)
- [Junos OS Editions on page 124](#)
- [FIPS 140-2 Security Compliance on page 125](#)
- [Junos OS Installation Packages on page 126](#)
- [Software Naming Convention on page 126](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)
- [Software Package Information Security on page 127](#)
- [Junos OS Release Numbers on page 128](#)
- [Configuration Files on page 129](#)

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. 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 123](#)
- [One Modular Software Architecture on page 124](#)

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.

Each new version of Junos OS software must include all working features released in previous releases of the software, and must have no critical regression errors. This discipline ensures reliable operations for the entire release.

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 124](#)
- [Junos OS Installation Packages on page 126](#)

Junos OS Editions

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 125](#).

- Related Documentation**
- [FIPS 140-2 Security Compliance on page 125](#)
 - [Software Naming Convention on page 126](#)
 - [Junos OS Release Numbers on page 128](#)

FIPS 140-2 Security Compliance

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**
- [Junos OS Editions on page 124](#)
 - [FIPS 140-2 Security Compliance on page 125](#)
 - [Software Naming Convention on page 126](#)
 - [Junos OS Release Numbers on page 128](#)

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:

Installation Package	Description
junos-srxsme*	Junos OS for all the branch SRX Series.
junos-srx1k3k*	Junos OS for SRX1400, SRX3400 and SRX3600.
junos-srx5000*	Junos OS for SRX 5600 and SRX5800.

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.

Related Documentation

- [Junos OS Editions on page 124](#)
- [FIPS 140-2 Security Compliance on page 125](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)
- [Junos OS Release Numbers on page 128](#)

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 128.



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-srxsme-10.0R1.8-domestic-tgz

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

Software Package Information Security

All Junos OS 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 133](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)

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 8.5, 9.1, or 9.2. 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 Web page, 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:

9.2R1.8

Where:

- *m* is the major 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
 - *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

Related Documentation

- [Junos OS Installation Packages on page 126](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)
- [Junos OS Editions on page 124](#)

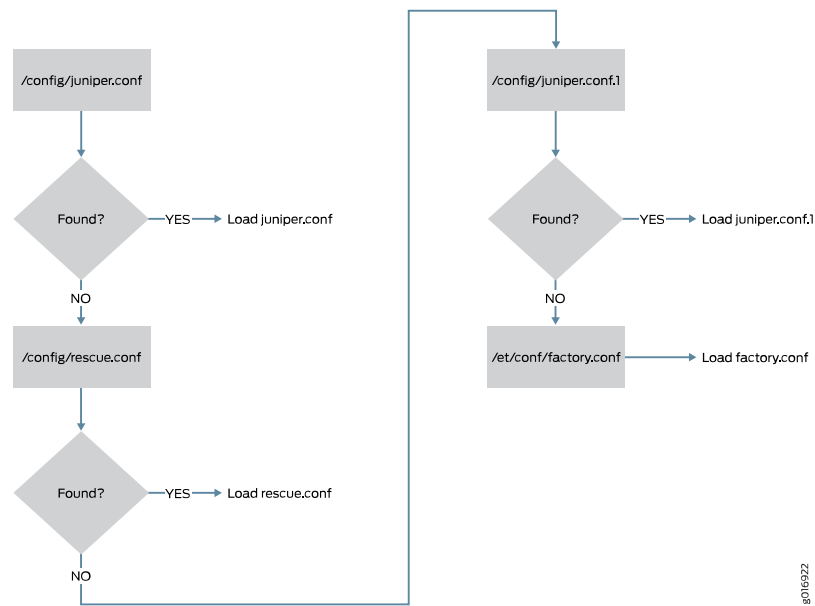
Configuration Files

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 5 on page 129](#).

Figure 5: 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 [“Load and Commit the Configuration File” on page 188](#).

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

- [Boot Sequence on SRX Series Devices on page 132](#)

Hardware Overview

- [Hardware Overview of SRX Series Services Gateways on page 130](#)
- [Storage Media Names for SRX Series Devices on page 132](#)
- [Boot Sequence on SRX Series Devices on page 132](#)

Hardware Overview of SRX Series Services Gateways

SRX Series Device Overview

[Figure 6 on page 131](#) shows an example of SRX240 device.

Figure 6: SRX240 Device Front Panel

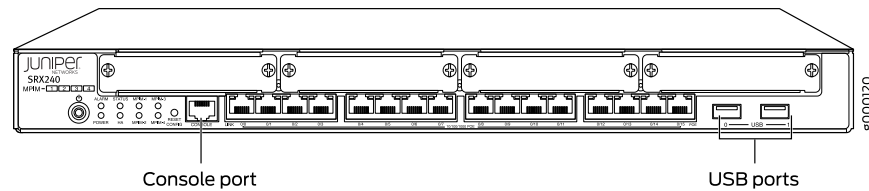


Figure 7 on page 131 shows an example of SRX650 device.

Figure 7: SRX650 Device System Routing Engine

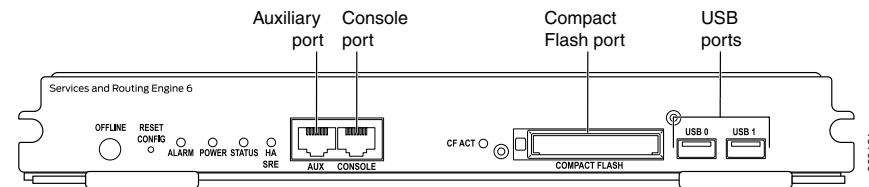
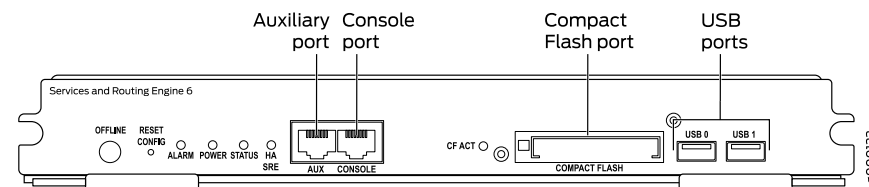


Figure 8 on page 131 shows an example of SRX5800 device Routing Engine.

Figure 8: SRX5800 Device Routing Engine



System Memory

The amount of free disk space necessary to upgrade a device with a new version of the 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 SRX100, SRX210, SRX240, Services Gateway can boot from the following storage media (in the order of priority):

- Internal NAND Flash (default; always present)
- USB storage key (alternate)

The SRX550 and SRX650 Services Gateway can boot from the following storage media (in the order of priority):

- CompactFlash (default; always present)

- External CompactFlash card (alternate) (SRX650 only)
- USB storage key (alternate)

SRX1400, SRX3400, SRX3600, 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 132](#)
- [Verifying PIC Combinations on page 137](#)

Storage Media Names for SRX Series Devices

Table 20 on page 132 specifies the storage media names used by the SRX Series devices. The storage media device names are displayed as the device boots.

Table 20: 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 130](#)
- [Boot Sequence on SRX Series Devices on page 132](#)

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
- USB storage media device

Related Documentation

- [Hardware Overview of SRX Series Services Gateways on page 130](#)
- [Storage Media Names for SRX Series Devices on page 132](#)

CHAPTER 6

Installing Junos OS Software

- [Installation Overview on page 133](#)
- [Performing a Standard or Change Category Installation on page 137](#)
- [Installing Software Using a USB Flash Drive on page 144](#)
- [Installing Software from the Boot Loader on page 147](#)
- [Configuring Automatic Installation of Configuration Files on page 151](#)
- [Configuring Dual-Root Partitions for High Availability on page 156](#)
- [Upgrading Software on page 166](#)
- [Booting a Device Using a System Snapshot on page 180](#)
- [Performing a Recovery Installation on page 183](#)
- [Rebooting or Halting Software Processes on a Device on page 188](#)
- [Configuring Administration User Accounts on page 193](#)

Installation Overview

- [Installation Type Overview on page 133](#)
- [Installation Categories on SRX Series Devices on page 134](#)
- [Understanding Download Manager for SRX Series Devices on page 135](#)

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 126](#).

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 126](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)

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 133](#)

- [Software Package Information Security on page 127](#)
- [Software Naming Convention for SRX Series Devices on page 126](#)

Understanding Download Manager for SRX Series Devices

This topic includes the following sections:

- [Overview on page 135](#)
- [Using Download Manager to Upgrade Junos OS on page 135](#)
- [Handling Errors on page 136](#)
- [Considerations on page 136](#)

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 21 on page 136](#) 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 21: 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 133](#)

Performing a Standard or Change Category Installation

- [Checking the Current Configuration and Candidate Software Compatibility on page 137](#)
- [Verifying PIC Combinations on page 137](#)
- [Determining the Junos OS Version on page 138](#)
- [Downloading Software on page 138](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Backing Up the Current Installation on SRX Series Devices on page 141](#)
- [Connecting to the Console Port on page 143](#)

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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)
- [request system snapshot \(Maintenance\) on page 273](#)
- [request system software add \(Maintenance\) on page 277](#)

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](#).

SRX3600 supports a maximum of up to seven SPCs, three NPCs, six IOCs, and 11 NP-IOCs per chassis. However you must install at least one SPCs and NPC on the chassis. SRX3400 supports a maximum of up to four SPCs, two NPCs, four IOCs, and six NP-IOCs per chassis. However you must install at least one SPCs and NPC on the chassis. On SRX3400 and SRX3600 devices you must install PICs on the front slots of the chassis. For more details, see [SR X1400, SRX3400, and SRX3600 Services Gateway Module 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 Web site at <http://www.juniper.net/support/>.

**Related
Documentation**

- [Hardware Overview of SRX Series Services Gateways on page 130](#)
- [Storage Media Names for SRX Series Devices on page 132](#)

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 170](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

Downloading Software

You can download the software in one of two ways:

- [Downloading Software with a Browser on page 139](#)
- [Downloading Software Using the Command-Line Interface on page 139](#)

Downloading Software with a Browser

You download the software package you need from the Juniper Networks Support Web site 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 Web site: <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 Web site 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 Web site: <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**
- [Connecting to the Console Port on page 143](#)
 - [Downloading Software Packages from Juniper Networks on page 141](#)
 - [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
 - [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

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 169](#)
 - [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
 - [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
 - [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

Backing Up the Current Installation on SRX Series Devices

This topic includes the following sections:

- [Backing Up the Current Installation on SRX High-End Devices on page 141](#)
- [Backing Up the Current Installation on Branch SRX Series Devices on page 142](#)
- [Configuring External CompactFlash for SRX650 Devices on page 142](#)

Backing Up the Current Installation on SRX High-End 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.
- **external**— Copies the snapshot to an external storage device. This option is available for the compact flash on the SRX650 Services Gateway

Configuring External CompactFlash for SRX650 Devices

Following procedure shows how to backup current installation on an SRX650 device.

The SRX650 Services Gateway includes the following 2 GB CompactFlash (CF) storage device:

- The Services and Routing Engine (SRE) contains a hot-pluggable external CF storage device used to upload and download files.
- The chassis contains an internal CF used to store the operating system.

By default, only the internal CF is enabled and an option to take a snapshot of the configuration from the internal CF to the external CF is not supported. This can be done only by using a USB storage device.

To take a snapshot of the configuration from the external CF:

1. Take a snapshot from the internal CF to a USB storage device using the **request system snapshot media usb** command.
2. Reboot the device from the USB storage device using the **request system reboot media usb** command.
3. Go to the U-boot prompt.
4. Stop at U-boot and set the following variables:


```
set ext.cf.pref 1
save
reset
```
5. Once the system is booted from the USB storage device, take a snapshot from the external CF using the **request system snapshot media external** command.



NOTE: Once the snapshot is taken on the external CF, we recommend that you set the `ext.cf.pref` to 0 at the U-boot prompt.

Related Documentation

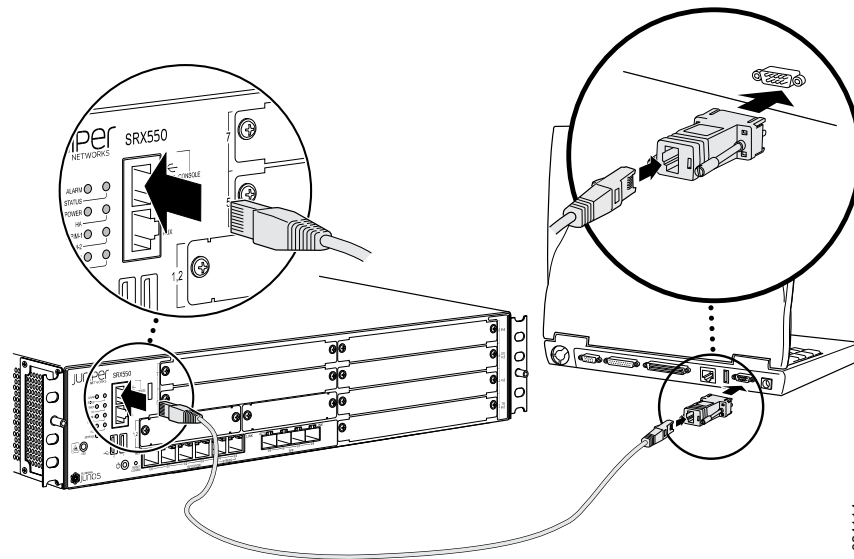
- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 148](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 150](#)

Connecting to the Console Port

The console port is a data terminal equipment (DTE) interface, providing a direct and continuous interface with the device. It is important to connect to the console during installation procedures so you can respond to any required user input and detect any errors that may occur.

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.

To configure the device initially, you must connect a terminal or laptop computer to the device through the console port, as shown in [Figure 9 on page 144](#).

Figure 9: Connecting to the Console Port on a Junos OS Device

9034114

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 [Hardware Documentation](#) for your particular device.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

Installing Software Using a USB Flash Drive

- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 144](#)
- [Installing Junos OS on SRX Series Devices Using a USB Flash Drive on page 146](#)

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.

You can use any USB flash drive device formatted with FAT/FAT 32 file systems for the installation process.



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.example.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 170](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

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

To install the Junos OS image on an SRX Series device:

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

If the LEDs do not turn amber, press the Power button or power-cycle the device and wait for the LEDs to steadily turn amber.

2. Press the Reset Config button on the SRX Series device and wait for the LEDs to turn green, indicating that the Junos OS upgrade image has 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: On all branch SRX Series devices, frequent plug and play of USB keys is not supported. You must wait for the device node creation before removing the USB key.



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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 144](#)
- [Backing Up the Current Installation on SRX Series Devices on page 141](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181](#)

Installing Software from the Boot Loader

- [Upgrading the Boot Loader on SRX Series Devices on page 147](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 148](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 150](#)

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 170](#)
- [Downloading Software Packages from Juniper Networks on page 141](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

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

You can install the Junos OS using the Trivial File Transfer Protocol (TFTP) method. The device is shipped with the Junos OS loaded on the primary boot device. During the 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 the 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 22 on page 149](#).

Table 22: 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.



NOTE: The Installation from the loader-over-TFTP method installs Junos OS on the internal CF on SRX100, SRX210, SRX220, and SRX240 devices, whereas on SRX650 devices, this method can install Junos OS on the internal or external CF card.

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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 144](#)
- [Backing Up the Current Installation on SRX Series Devices on page 141](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181](#)

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.

Related Documentation

- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 144](#)
- [Backing Up the Current Installation on SRX Series Devices on page 141](#)
- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181](#)

Configuring Automatic Installation of Configuration Files

- [Autoinstallation Overview on page 151](#)
- [Configuring Autoinstallation on SRX Series Devices on page 154](#)

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:

- [Supported Autoinstallation Interfaces and Protocols on page 152](#)
- [Typical Autoinstallation Process on a New Device on page 152](#)

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 23 on page 152](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 23: 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)
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 154](#)

Configuring Autoinstallation on SRX Series Devices

This example shows how to configure a device for autoinstallation.

- [Requirements on page 154](#)
- [Overview on page 154](#)
- [Configuration on page 154](#)
- [Verification on page 156](#)

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. See [“Example: Configuring the Device as a DHCP Server” on page 929](#).
- Create one of the following configuration files, and store it on a TFTP server in the network (see [“Configuration Files” on page 129](#)):
 - 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 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 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*.

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 system 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 HDLC 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 156](#)

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 151](#)

Configuring Dual-Root Partitions for High Availability

- [Dual-Root Partitioning Scheme on SRX Series Devices on page 156](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 162](#)
- [Reinstalling the Single-Root Partition on SRX Series Devices on page 165](#)

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 157](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 158](#)
- [Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning on page 158](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers Devices on page 160](#)
- [Understanding How Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on page 161](#)

[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 24 on page 157](#) provides information on the storage media available on SRX Series devices.

Table 24: Storage Media on SRX Series Devices

SRX Series Devices	Storage Media
SRX100, SRX210, and SRX240	<ul style="list-style-type: none"> • Internal NAND flash (default; always present) • USB storage device (alternate)
SRX110, SRX220	<ul style="list-style-type: none"> • CompactFlash (default; always present) • USB storage device (alternate)
SRX550	<ul style="list-style-type: none"> • Internal CF (default; always present) • USB storage device (alternate)

Table 24: Storage Media on SRX Series Devices (*continued*)

SRX Series Devices	Storage Media
SRX650	<ul style="list-style-type: none"> Internal CF (default; always present) External flash card (alternate) USB storage device (alternate)

With the dual-root partitioning scheme, the SRX Series device first tries to boot the 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 the 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.

```
login: user
```

```
Password:
```

```
*****
```

```
**
```

```
**
```

```
** 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.      **
**                                                                    **
** The primary copy will be recovered by auto-snapshot feature now.    **
**                                                                    **
*****

```

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.
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 148](#)
- 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 150](#)

- 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 169](#)
- [Reinstalling the Single-Root Partition on SRX Series Devices on page 165](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 162](#)

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 162](#)
- [Overview on page 162](#)
- [Configuration on page 163](#)
- [Verification on page 165](#)

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 SRX100, SRX210, and SRX240 devices (internal NAND flash) and on SRX650 devices (internal CF card).

Partition install is *not* supported on the alternate media on SRX100, SRX210, and SRX240 devices (USB storage key) or on SRX650 devices (external CF card or 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 in a text file, remove any line breaks, 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* 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 144.
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 165](#)

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 156](#)
- [Reinstalling the Single-Root Partition on SRX Series Devices on page 165](#)

Reinstalling the Single-Root Partition on SRX Series Devices

Junos OS Release 9.6 and earlier is not compatible with the dual-root partitioning scheme. These releases can only be installed if the media is reformatted with single-root partitioning. Any attempt to install Junos OS Release 9.6 or earlier on a device with dual-root partitioning without reformatting the media will fail with an error. You must install the Junos OS Release 9.6 or earlier image from the boot loader using a TFTP server or USB storage device.



NOTE: Junos OS Release 12.1X45 and later do not support single root partitioning.



NOTE: You do not need to reinstall the earlier version of the boot loader if you are installing the Junos OS Release 9.6.

You cannot install a Junos OS Release 9.6 or earlier package on a system with dual-root partitioning using the Junos OS CLI or J-Web. If this is attempted, an error will be returned.

You can install the Junos OS Release 9.6 (9.6R3 and 9.6R4 [only]) on a system with dual-root partitioning using **request system software add** command with **partition** option.

To reinstall the single-root partition:

1. Enter the request system software add partition command to install the previous Junos OS version (9.6R3 and 9.6R4):

```
user@host>request system software add partition
```

2. Reboot the device

```
user@host>request system reboot
```

The previous software version gets installed after rebooting the device.



NOTE: Using the `request system software add` CLI command with the `partition` option to install Junos OS Release 9.6 (9.6R3 and 9.6R4) reformats the media with single-root partitioning. This process erases the dual-root partitioning scheme from the system, so the benefits of dual-root partitioning will no longer be available.

**Related
Documentation**

- [Dual-Root Partitioning Scheme on SRX Series Devices on page 156](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 162](#)

Upgrading Software

- [Upgrading Individual Software Packages on page 167](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 176](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 178](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 178](#)

Upgrading Individual 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.)

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/>. Choose either the Canada and U.S. Version or the Worldwide Version.

To download the software packages, 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 Web site: <https://www.juniper.net/registration/Register.jsp>.



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.

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:

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

installation-package is the full URL to the file.



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 is 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.

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
```

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
```

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.

- Related Documentation**
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
 - [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)

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.

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 126](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

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 on page 171](#)
- [Verifying Available Disk Space on SRX Series Devices on page 171](#)
- [Cleaning Up the System File Storage Space on page 172](#)

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 25 on page 171 lists the secondary storage devices available on an SRX Series devices.

Table 25: Secondary Storage Devices for SRX Series Devices

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX100, SRX110, SRX210, SRX220, and SRX240 Services Gateways	1 GB
	SRX550, and SRX650 Services Gateway	2 GB
External CompactFlash (CF)	SRX650 Services Gateway	2 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 the 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 the 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.

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 173](#)
- [Overview on page 173](#)
- [Configuration on page 174](#)
- [Verification on page 175](#)

Requirements

Before you begin:

- Verify the available space on the internal media. See [“Preparing Your SRX Series Device for Junos OS Upgrades” on page 170](#) and the *Junos OS Release Notes*
- Download the software package. See [“Downloading Software Packages from Juniper Networks” on page 141](#).
- 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 install Junos OS upgrades on SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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* 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 175](#)

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 169](#)
 - [Preparing the USB Flash Drive to Upgrade Junos OS on SRX Series Devices on page 144](#)
 - [Preparing Your SRX Series Device for Junos OS Upgrades on page 170](#)
 - [Downloading Software Packages from Juniper Networks on page 141](#)
 - [Configure Administration User Accounts on page 193](#)

Installing Junos OS Upgrade Packages on SRX 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 170](#) and the *Junos OS Release Notes*
- Download the software package. See [“Downloading Software Packages from Juniper Networks” on page 141](#).

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 26 on page 176](#).

Table 26: 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 173](#)
- [Configure Administration User Accounts on page 193](#)

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 SRX240 and SRX650 Service Gateways also include a U-shell binary as part of the BIOS. Additionally, on SRX100, SRX110, SRX210, SRX220 and SRX240 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 27 on page 177](#) Lists the CLI commands used for manual BIOS upgrade.

Table 27: 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.



NOTE: The SRX650 device has only one set of BIOS. There is no backup BIOS upgrade for the SRX650 device.

Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a TFTP Server on page 148](#)
- [Installing Junos OS on SRX Series Devices from the Boot Loader Using a USB Storage Device on page 150](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 178](#)

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 169](#)
- [Understanding BIOS Upgrades on SRX Series Devices on page 176](#)

Example: Downgrading Junos OS on SRX Series Devices

This example shows how to downgrade Junos OS on the SRX Series devices.

- [Requirements on page 179](#)
- [Overview on page 179](#)

- [Configuration on page 179](#)
- [Verification on page 180](#)

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 downgrade Junos OS on SRX Series devices, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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*.

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 180](#)

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 181](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Restarting and Halting SRX Series Devices on page 189](#)

Booting a Device Using a System Snapshot

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181](#)

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 181](#)
- [Overview on page 181](#)
- [Configuration on page 181](#)
- [Verification on page 182](#)

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 170](#).

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 a boot device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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*.

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 183](#)

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 170](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 169](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)

Performing a Recovery Installation

- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 184](#)
- [Saving a Rescue Configuration File on page 186](#)
- [Restoring a Saved Configuration on page 187](#)

Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices

This topic includes the following sections:

- [Overview on page 184](#)
- [How Autorecovery Works on page 184](#)
- [How to Use Autorecovery on page 184](#)
- [Data That Is Backed Up in an Autorecovery on page 185](#)
- [Troubleshooting Alarms on page 185](#)
- [Considerations on page 185](#)

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 28 on page 185 lists types of autorecovery alarms, descriptions, and required actions.

Table 28: 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 bootup.
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 181](#)
- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 178](#)

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 the [Junos System Basics: Getting Started Configuration Guide](#).

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
```

Related Documentation

- [Restoring a Saved Configuration on page 187](#)
- [Restoring a Saved Configuration on page 187](#)

Restoring a Saved Configuration

To restore a saved configuration, perform the following tasks:

1. [Copy Saved Files to the Router on page 187](#)
2. [Load and Commit the Configuration File on page 188](#)

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 l.  
ftp> get /path/file  
ftp> bye  
Goodbye.
```

Load and Commit 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@routename> 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).

Related Documentation

- [Saving a Rescue Configuration File on page 186](#)

Rebooting or Halting Software Processes on a Device

- [Restarting and Halting SRX Series Devices on page 189](#)

Restarting and Halting SRX Series Devices

This topic includes the following sections:

- [Rebooting SRX Series Devices on page 189](#)
- [Halting SRX Series Devices on page 190](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 192](#)
- [Restarting the Chassis on SRX Series Devices on page 192](#)

Rebooting SRX Series Devices

This example shows how to reboot a SRX Series device.

- [Requirements on page 189](#)
- [Overview on page 189](#)
- [Configuration on page 189](#)
- [Verification on page 190](#)

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 reboot a device, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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* 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 190](#)

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 191](#)
- [Overview on page 191](#)
- [Configuration on page 191](#)
- [Verification on page 192](#)

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 halt a device immediately, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

From operational mode, enter:

```
user@host>request system halt at now
```

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* 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 192](#)

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 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 (for SRX Series devices):

- **cluster**—Changes the chassis cluster status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.

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
```

Configuring Administration User Accounts

- [Configure Administration User Accounts on page 193](#)

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
```

Related Documentation

- [Example: Installing Junos OS Upgrade Packages on SRX Series Devices on page 173](#)
- [Installing Junos OS Upgrade Packages on SRX Devices from a Remote Server on page 175](#)

CHAPTER 7

Installing and Managing Software Licenses

- [Software Licenses Overview on page 195](#)
- [Installing and Managing Licenses on page 208](#)

Software Licenses Overview

- [Junos OS Feature Licenses on page 195](#)
- [License Enforcement on page 196](#)
- [Junos OS Feature License Keys on page 196](#)
- [Software Feature Licenses for SRX Series Devices on page 198](#)

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 196](#)
- [Working with License Keys for SRX Series Devices on page 209](#)
- [Junos OS Feature License Model Number for SRX Series Services Gateways on page 198](#)

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 License Keys on page 196](#)
- [Junos OS Feature License Model Number for SRX Series Services Gateways on page 198](#)
- [Working with License Keys for SRX Series Devices on page 209](#)

Junos OS Feature License Keys

This section contains the following topics:

- [License Key Components on page 197](#)
- [License Management Fields Summary on page 197](#)

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 29 on page 197](#).

Table 29: 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.

Table 29: Summary of License Management Fields (*continued*)

Field Name	Definition
Group	<p>If the license defines a group license, this field displays the group definition.</p> <p>If the license requires a group license, this field displays the required group definition.</p> <p>NOTE: Because group licenses are currently unsupported, this field is always blank.</p>
Enabled Features	Name of the feature that is enabled with the particular license.
Expiry	<p>Verify that the expiration information for the license is correct.</p> <p>For Junos OS, only permanent licenses are supported. If a license has expired, it is shown as invalid.</p>

- Related Documentation**
- [Generating a License Key on page 209](#)
 - [Updating License Keys on page 210](#)
 - [Saving License Keys on page 210](#)
 - [Downloading License Keys on page 209](#)

Software Feature Licenses for SRX Series Devices

Table 30: Junos OS Feature Licenses

Junos OS License Requirements										
Feature	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
Access Manager	X	X	X	X	X	X	X			
BGP Route Reflectors							X			
Dynamic VPN	X	X	X	X	X	X	X			
IDP Signature Update*	X *	X	X *	X *	X *	X	X	X	X	X
Application Signature Update (Application Identification)*	X	X	X	X	X	X	X	X	X	X
Juniper-Kaspersky Antivirus*	X	X	X	X	X	X	X			
Juniper-Sophos Antivirus*	X	X	X	X	X	X	X	X	X	X

Table 30: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements										
Feature	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
Juniper-Sophos Antispam*	X	X	X	X	X	X	X	X	X	X
Juniper-Enhanced Web filtering*	X	X	X	X	X	X	X	X	X	X
Juniper-Websense Web filtering*	X	X	X	X	X	X	X			
Logical Systems								X	X	X
SRX100 Memory Upgrade	X									

* Indicates support on high-memory devices only.

Table 31 on page 200 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 31: 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)	SRX100	SRX100-APPSEC-A-1
		SRX100-APPSEC-A-3
		SRX100-APPSEC-A-5
	SRX210, SRX220, and SRX240	SRX2XX-APPSEC-A-1
		SRX2XX-APPSEC-A-3
		SRX2XX-APPSEC-A-5
	SRX550	SRX550-APPSEC-A-1
		SRX550-APPSEC-A-3
		SRX550-APPSEC-A-5
	SRX650	SRX650-APPSEC-A-1
		SRX650-APPSEC-A-3
		SRX650-APPSEC-A-5
	SRX1400	SRX1400-APPSEC-A-1
		SRX1400-APPSEC-A-3
		SRX1400-APPSEC-A-1-R
		SRX1400-APPSEC-A-3-R
	SRX3400	SRX3400-APPSEC-A-1
		SRX3400-APPSEC-A-3
	SRX3600	SRX3600-APPSEC-A-1
		SRX3600-APPSEC-A-3
	SRX5400	SRX5400-APPSEC-1
		SRX5400-APPSEC-3
		SRX5400-APPSEC-5
	SRX5600	SRX5600-APPSEC-A-1
		SRX5600-APPSEC-A-3
		SRX5600-APPSEC-A-5
	SRX5800	

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
IDP updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX5800-APPSEC-A-1
		SRX5800-APPSEC-A-3
		SRX5800-APPSEC-A-5
	SRX100, SRX110	SRX1XX-IDP
		SRX1XX-IDP-3
		SRX1XX-IDP-5
	SRX210, SRX220, SRX240	SRX2XX-IDP
		SRX2XX-IDP-3
		SRX2XX-IDP-5
	SRX550	SRX550-IDP
		SRX550-IDP-3
		SRX550-IDP-5
	SRX650	SRX650-IDP
		SRX650-IDP-3
		SRX650-IDP-5
IDP subscription (1 year and 3 years)	SRX3400, SRX3600	SRX3K-IDP
		SRX3K-IDP-3
	SRX5400, SRX5600, SRX5800	SRX5K-IDP
		SRX5K-IDP-3
		SRX5K-IDP-3-R
		SRX5K-IDP-R
	SRX5400, SRX5600, SRX5800	SRX5K-IDP
		SRX5K-IDP-3

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-K-AV
		SRX1XX-K-AV-3
		SRX1XX-K-AV-5
	SRX210, SRX220, SRX240	SRX2XX-K-AV
		SRX2XX-K-AV-3
		SRX2XX-K-AV-5
	SRX550	SRX550-K-AV
		SRX550-K-AV-3
		SRX550-K-AV-5
	SRX650	SRX650-K-AV
		SRX650-K-AV-3
		SRX650-K-AV-5
Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years)	SRX100, SRX110	SRX1XX-S-AV
		SRX1XX-S-AV-3
		SRX1XX-S-AV-5
	SRX210, SRX220, SRX240	SRX2XX-S-AV
		SRX2XX-S-AV-3
		SRX2XX-S-AV-5
	SRX550	SRX550-S-AV
		SRX550-S-AV-3
		SRX550-S-AV-5
	SRX650	SRX650-S-AV
		SRX650-S-AV-3
		SRX650-S-AV-5

Table 31: 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)	SRX1400	SRX1400-S-AV-1
		SRX1400-S-AV-3
		SRX1400-S-AV-5
	SRX3400	SRX3400-S-AV-1
		SRX3400-S-AV-3
		SRX3400-S-AV-5
	SRX3600	SRX3600-S-AV-1
		SRX3600-S-AV-3
		SRX3600-S-AV-5
	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)	SRX100, SRX110	SRX1XX-S2-AS
		SRX1XX-S2-AS-3
		SRX1XX-S2-AS-5
	SRX210, SRX220, SRX240	SRX2XX-S2-AS
		SRX2XX-S2-AS-3
		SRX2XX-S2-AS-5
	SRX550	SRX550-S2-AS
		SRX550-S2-AS-3
		SRX550-S2-AS-5
	SRX650	SRX650-S2-AS
		SRX650-S2-AS-3
		SRX650-S2-AS-5

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years)	SRX1400	SRX1400-S-AV-1
		SRX1400-S-AV-3
		SRX1400-S-AV-5
	SRX3400	SRX3400-S-AV-1
		SRX3400-S-AV-3
		SRX3400-S-AV-5
	SRX3600	SRX3600-S-AV-1
		SRX3600-S-AV-3
		SRX3600-S-AV-5
	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)	SRX100, SRX110	SRX1XX-W-EWF
		SRX1XX-W-EWF-3
		SRX1XX-W-EWF-5
	SRX210, SRX220, SRX240	SRX2XX-W-EWF
		SRX2XX-W-EWF-3
		SRX2XX-W-EWF-5
	SRX550	SRX550-W-EWF
		SRX550-W-EWF-3
		SRX550-W-EWF-5
	SRX650	SRX650-W-EWF
		SRX650-W-EWF-3
		SRX650-W-EWF-5

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years)	SRX1400	SRX1400-W-EWF-1
		SRX1400-W-EWF-3
		SRX1400-W-EWF-5
	SRX3400	SRX3400-W-EWF-1
		SRX3400-W-EWF-3
		SRX3400-W-EWF-5
	SRX3600	SRX3600-W-EWF-1
		SRX3600-W-EWF-3
		SRX3600-W-EWF-5
	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)	SRX100, SRX110	SRX1XX-SMB4-CS
		SRX1XX-SMB4-CS-3
		SRX1XX-SMB4-CS-5
	SRX210, SRX220, SRX240	SRX2XX-SMB4-CS
		SRX2XX-SMB4-CS-3
		SRX2XX-SMB4-CS-5
	SRX550	SRX550-SMB4-CS
		SRX550-SMB4-CS-3
		SRX550-SMB4-CS-5
	SRX650	SRX650-SMB4-CS
		SRX650-SMB4-CS-3
		SRX650-SMB4-CS-5

Table 31: 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)	SRX100, SRX110	SRX1XX-S-SMB4-CS
		SRX1XX-S-SMB4-CS-3
		SRX1XX-S-SMB4-CS-5
	SRX210, SRX220, SRX240	SRX2XX-S-SMB4-CS
		SRX2XX-S-SMB4-CS-3
		SRX2XX-S-SMB4-CS-5
	SRX550	SRX550-S-SMB4-CS
		SRX550-S-SMB4-CS-3
		SRX550-S-SMB4-CS-5
	SRX650	SRX650-S-SMB4-CS
		SRX650-S-SMB4-CS-3
		SRX650-S-SMB4-CS-5
Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years)	SRX1400	SRX1400-CS-BUN-1
		SRX1400-CS-BUN-3
		SRX1400-CS-BUN-5
	SRX3400	SRX3400-CS-BUN-1
		SRX3400-CS-BUN-3
		SRX3400-CS-BUN-5
	SRX3600	SRX3600-CS-BUN-1
		SRX3600-CS-BUN-3
		SRX3600-CS-BUN-5
	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

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Dynamic VPN Client (5, 10, and 25 simultaneous users)	SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650	SRX-RAC-5-LTU
		SRX-RAC-10-LTU
		SRX-RAC-25-LTU
Dynamic VPN Service (5, 10, 25, and 50 simultaneous users)	SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550	SRX-RAC-5-LTU
	SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550	SRX-RAC-10-LTU
	SRX210, SRX240, SRX100, SRX220, SRX650, SRX550	SRX-RAC-25-LTU
	SRX240, SRX650, SRX220, SRX210, SRX550	SRX-RAC-50-LTU
Dynamic VPN Service (100 and 150 simultaneous users)	SRX650, SRX220, SRX240, SRX550	SRX-RAC-100-LTU
		SRX-RAC-150-LTU
Dynamic VPN Service (250 simultaneous users)	SRX650, SRX240, SRX550 NOTE: Requires Junos OS 11.2R3 or later	SRX-RAC-250-LTU
Dynamic VPN Service (500 simultaneous users)	SRX650, SRX550 NOTE: Requires Junos OS 11.2R3 or later	SRX-RAC-500-LTU
Express Path License (formerly known as <i>services offloading</i>) 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.	SRX1400	SRX1K-SVCS-OFFLOAD-RTU
	SRX3400, SRX3600	SRX3K-SVCS-OFFLOAD-RTU
	SRX5400, SRX5600, SRX5800	SRX5K-SVCS-OFFLOAD-RTU
Memory Software License (Upgrades SRX100B model from 512-MB RAM to 1-GB RAM)	SRX100	SRX100-MEM-LIC-UPG
Advanced BGP License	SRX650 only	SRX-BGP-ADV-LTU

Table 31: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

Licensed Software Feature	Supported Devices	Model Number
Logical Systems License (incremental 1, 5, and 25 numbers)	SRX1400	SRX-1400-LSYS-1
		SRX-1400-LSYS-25
		SRX-1400-LSYS-5
	SRX3400	SRX-3400-LSYS-1
		SRX-3400-LSYS-5
		SRX-3400-LSYS-25
	SRX3600	SRX-3600-LSYS-1
		SRX-3600-LSYS-5
		SRX-3600-LSYS-25
	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

- Related Documentation**
- [License Enforcement on page 196](#)
 - [Junos OS Feature License Keys on page 196](#)
 - [Working with License Keys for SRX Series Devices on page 209](#)

Installing and Managing Licenses

- [Working with License Keys for SRX Series Devices on page 209](#)

Working with License Keys for SRX Series Devices

This topic includes the following sections:

- [Generating a License Key on page 209](#)
- [Downloading License Keys on page 209](#)
- [Displaying License Keys in J-Web on page 209](#)
- [Saving License Keys on page 210](#)
- [Updating License Keys on page 210](#)
- [Example: Adding a New License Key on page 210](#)
- [Example: Deleting a License Key on page 213](#)

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.

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.

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.

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
```

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://ael.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
```

Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 210](#)
- [Overview on page 211](#)
- [Configuration on page 211](#)
- [Verification on page 212](#)

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 add a new license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

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.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

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 on page 212](#)
- [Verifying License Usage on page 213](#)
- [Verifying Installed License Keys on page 213](#)

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.

Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 213](#)
- [Overview on page 213](#)
- [Configuration on page 214](#)
- [Verification on page 214](#)

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 delete a license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
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**.



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

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
```



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

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 214](#)

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

- [Software Feature Licenses for SRX Series Devices on page 198](#)

CHAPTER 8

Configuration Statements and Operational Commands

- [Configuration Statements on page 217](#)
- [Operational Commands on page 258](#)

Configuration Statements

- [System Configuration Statement Hierarchy on page 217](#)
- [auto-configuration on page 248](#)
- [auto-configuration \(System\) on page 249](#)
- [autoinstallation on page 251](#)
- [bootp on page 252](#)
- [commit on page 253](#)
- [configuration-servers on page 254](#)
- [interfaces \(Autoinstallation\) on page 255](#)
- [license on page 256](#)
- [usb on page 258](#)
- [usb-control on page 258](#)

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 passsword;
  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-rollbacks 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;
        }
    }
    traceoptions {
        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;
    traceoptions {
        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;  
}
```

Related Documentation • [Security Configuration Statement Hierarchy on page 57](#)

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 151• Configuring Autoinstallation on SRX Series Devices on page 154

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 151• Configuring Autoinstallation on SRX Series Devices on page 154 |
|------------------------------|--|

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 154

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">• Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 944

commit

Syntax	<pre> commit { server { commit-interval <i>seconds</i>; days-to-keep-error-logs <i>days</i>; maximum-aggregate-pool <i>number</i>; maximum entries <i>number</i>; traceoptions { file { <i>filename</i>; files <i>number</i>; microsecond-stamp; size <i>maximum-file-size</i>; (world-readable no-world-readable); } flag <i>flag</i>; no-remote-trace; } } synchronize; } </pre>
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	<ul style="list-style-type: none"> <i>Controlling Execution of Commit Scripts During Commit Operations</i>

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 154

interfaces (Autoinstallation)

Syntax	<pre>interfaces { <i>interface-name</i> { 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.
Options	<ul style="list-style-type: none">• bootp—Enables BOOTP or DHCP during autoinstallation.• rarp—Enables RARP during autoinstallation.
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 151• Configuring Autoinstallation on SRX Series Devices on page 154

license

```
Syntax  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;
        }
    }
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify license information for the device.

- Options
- **autoupdate**—Autoupdate license keys from license servers.
 - **url**—URL of a license server.
 - **renew**—License renewal lead time and checking interval.
 - **before-expiration *number***—License renewal lead time before expiration in days.
Range : 0 through 60 days
 - **interval *interval-hours***—License checking interval in hours.
Range : 1 through 336 hours
 - **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 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 **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	<ul style="list-style-type: none">• Junos OS Feature License Keys on page 196
------------------------------	---

usb

Syntax	<code>usb { disable; }</code>
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 154

usb-control


Syntax	<code>usb-control { 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 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.
Related Documentation	<ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217

Operational Commands

- [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 update
- request system power-off
- request system snapshot (Maintenance)
- request system software abort in-service-upgrade (ICU)
- request system software add (Maintenance)
- request system software reboot
- request system software rollback (Maintenance)
- show chassis usb storage
- show system auto-snapshot
- show system autorecovery state
- show system download
- show system license (View)
- show system snapshot media
- show system storage (View SRX Series)
- show system storage partitions (View SRX Series)
- show version

request system autorecovery state

Syntax	request system autorecovery state (save recover clear)
Release Information	Command introduced in Junos OS Release 11.2.
Description	Prepares 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 283
List of Sample Output	request system autorecovery state save on page 261 request system autorecovery state recover on page 261 request system autorecovery state clear on page 261
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.
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 command until a 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 paused.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system download start on page 266• request system download pause on page 264• request system download resume on page 265• request system download clear on page 263
List of Sample Output	request system download abort on page 262
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.
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 266• request system download pause on page 264• request system download resume on page 265• request system download abort on page 262
List of Sample Output	request system download clear on page 263
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.
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 266• request system download resume on page 265• request system download abort on page 262• request system download clear on page 263
List of Sample Output	request system download pause on page 264
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.
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	<p>download-id—(Required) The ID number of the download to be paused.</p> <p>max-rate—(Optional) The maximum bandwidth for the download.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system download start on page 266 • request system download pause on page 264 • request system download abort on page 262 • request system download clear on page 263
List of Sample Output	request system download resume on page 265
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.
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 264• request system download resume on page 265• request system download abort on page 262• request system download clear on page 263
List of Sample Output	request system download start on page 266
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	<code>request system firmware upgrade</code>
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 90
List of Sample Output	request system firmware upgrade on page 267
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 271
List of Sample Output	request system halt on page 268
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 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 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 115
List of Sample Output	request system license update on page 270 request system license update trial on page 270
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

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 268
List of Sample Output	request system power-off on page 271
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 `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 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 snapshot (Maintenance)

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**
- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
 - **media**— (Optional) Specifies the media to be included in the snapshot:
 - **compact-flash**— Copies the snapshot to an external compact flash.
 - **hard-disk**— Copies the snapshot to a hard disk.
 - **usb**— Copies the snapshot to the USB storage device.
 - **internal**— Copies the snapshot to internal media. This is the default.



NOTE: USB option is available on all SRX series devices; hard disk and compact-flash options are available only on high-end SRX series devices; media internal option is available only on branch SRX series devices.

- **node**— (Optional) Specifies to archive the data and executable areas of a specific node.
 - **node-id**—Archive a specific node. The range of node ID is (0,1)
 - **all**—Archive all nodes.
 - **local**—Archive only local nodes.
 - **primary**—Archive only 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.
- You cannot partition a hard-disk as it is mounted on /var directory.

- 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.
- The slice partition is supported only on branch SRX Series devices.

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 162
List of Sample Output	request system snapshot media hard-disk on page 274 request system snapshot media usb (when usb device is missing on page 274 request system snapshot media compact-flash on page 275 request system snapshot media internal on page 275 request system snapshot partition on page 275
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 (dals1a)...
```



```
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 media internal

```
user@host> request system snapshot media internal
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 276
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	Installs 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 save 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 software reboot on page 278

request system software reboot

Syntax	<code>request system software reboot <at time> <in minutes><media><message 'text'></code>
Release Information	Command introduced in Junos OS Release 10.1.
Description	Reboots the software.
Options	<ul style="list-style-type: none">• at time— Specifies the time at which to reboot the device . You can specify time in one of the following ways:<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">• internal— Reboots from the internal media. This is the default.• usb— Reboots from the USB storage device.• external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.• message "text"— Provides a message to display to all system users before the device reboots. <p>Example: request system reboot at 5 in 50 media internal message stop</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system software rollback (Maintenance) on page 279

request system software rollback (Maintenance)

Syntax	request system software rollback
Release Information	Command introduced in Junos OS Release 10.1.
Description	Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system software reboot on page 278

show chassis usb storage

Syntax	show chassis usb storage
Release Information	Command introduced in Junos OS Release 11.4 R2.
Description	Displays 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 146
List of Sample Output	show chassis hardware detail on page 280 show chassis usb storage on page 280

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 auto-snapshot

Syntax	show system auto-snapshot
Release Information	Command introduced in Junos OS Release 12.1X45-D10.
Description	<p>Display the status of the auto-snapshot information on SRX Series devices. 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 to 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.</p> <p>When the automatic snapshot procedure is in progress, you cannot run the manual snapshot command, request system snapshot.</p>
Required Privilege Level	View
Related Documentation	<ul style="list-style-type: none"> • show system snapshot media on page 290 • Example: Creating a Snapshot and Using It to Boot an SRX Series Device on page 181
List of Sample Output	show system auto-snapshot on page 282
Output Fields	<p>Table 32 on page 281 lists the output fields for the show system auto-snapshot command. Output fields are listed in the approximate order in which they appear.</p>

Table 32: show system auto-snapshot Output Fields

Field Name	Field Description
Auto-snapshot Configuration	<p>Displays the configuration status of auto-snapshot.</p> <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 to 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 to the other.
Auto-snapshot State	<p>Displays the current state of auto-snapshot.</p> <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@host> show system auto-snapshot
```

```
Auto-snapshot Configuration:  Enabled
Auto-snapshot State: Completed
```


show system autorecovery state

Syntax	show system autorecovery state
Release Information	Command introduced in Junos OS Release 11.2.
Description	Performs checks and shows status of all autorecovered items.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request system autorecovery state on page 260 • Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 184
List of Sample Output	show system autorecovery state on page 283
Output Fields	Table 33 on page 283 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear.

Table 33: 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 download

Syntax	<code>show system download <download-id></code>
Release Information	Command introduced in Junos OS Release 11.2.
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 266 Understanding Download Manager for SRX Series Devices on page 135
List of Sample Output	show system download on page 285 show system download 1 on page 286
Output Fields	Table 34 on page 285 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear.

Table 34: 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 location of the downloaded file.

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"> • Working with License Keys for SRX Series Devices on page 209
List of Sample Output	<p>show system license on page 288</p> <p>show system license installed on page 288</p> <p>show system license keys on page 289</p> <p>show system license usage on page 289</p> <p>show system license status logical-system all on page 289</p>
Output Fields	Table 18 on page 115 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.

Table 35: 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 35: 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 xxx
```

show system license usage

```
user@host> show system license usage
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine	1	1	0	2012-03-30
01:00:00 IST				
wf_key_surfcontrol_cpa	0	1	0	2012-03-30
01:00:00 IST				
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 snapshot media

Syntax	show system snapshot media <i>media-type</i>
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">• internal— Show snapshot information from internal media.• usb— Show snapshot information from device connected to USB port.• external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.
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 181

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/da1s1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/da1s2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```


show system storage (View SRX Series)

Syntax show system storage
 <detail>
 <node *node-id* | all | local | primary>
 <partitions>

Release Information Command introduced in Junos OS Release 10.2.

Description Display the local storage data currently available on the SRX Series devices.

- Options**
- **none**—Display standard information about the amount of free disk space in the device file system.
 - **detail**—(Optional) Display detailed output about the amount of free disk space in the device file system.
 - **node**—(Optional) Display local storage data for a specific node.



NOTE: The **node** option is supported only on high-end SRX Series devices.

- **node-id**—Identification number of the node. It can be 0 or 1.
- **all**—(Optional) Display the local storage data for all nodes.
- **local**—(Optional) Display the local storage data for the local node.
- **primary**—(Optional) Display the local storage data for the primary node.
- **partitions**—(Optional) Display partitions information for the boot media.



NOTE: The **partitions** option is supported only on branch SRX Series devices.

Required Privilege Level View

Output Fields [Table 36 on page 291](#) describes the output fields for the **show system storage** command. Output fields are listed in the approximate order in which they appear.

Table 36: show system storage Output Fields

Field Name	Field Description
Filesystem	Name of the file system.
Size	Size of the file system.
Used	Amount of space used in the file system.

Table 36: show system storage Output Fields (*continued*)

Field Name	Field Description
Avail	Amount of space available in the file system.
Capacity	Percentage of the file system space that is being used.
Mounted on	Directory in which the file system is mounted.

show system storage

```
user@host>show system storage
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s2a	621M	169M	402M	30%	/
devfs	1.0K	1.0K	0B	100%	/dev
/dev/md0	20M	6.3M	12M	35%	/junos
/cf/packages	621M	169M	402M	30%	/junos/cf/packages
devfs	1.0K	1.0K	0B	100%	/junos/cf/dev
/dev/md1	494M	494M	0B	100%	/junos
/cf	20M	6.3M	12M	35%	/junos/cf
devfs	1.0K	1.0K	0B	100%	/junos/dev/
/cf/packages	621M	169M	402M	30%	/junos/cf/packages
1					
procfs	4.0K	4.0K	0B	100%	/proc
/dev/bo0s3e	49M	24K	45M	0%	/config
/dev/bo0s3f	616M	399M	168M	70%	/cf/var
/dev/md2	336M	20M	289M	7%	/mfs
/cf/var/jail	616M	399M	168M	70%	/jail/var
/cf/var/log	616M	399M	168M	70%	/jail/var/log
devfs	1.0K	1.0K	0B	100%	/jail/dev
/dev/md3	63M	4.0K	58M	0%	/mfs/var/run/utm
/dev/md4	1.8M	228K	1.5M	13%	/jail/mfs

show system storage partitions (View SRX Series)

Syntax	show system storage partitions
Release Information	Command introduced in Junos OS Release 10.2 .
Description	Displays 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 162

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
```


show version

Syntax	show version <brief detail> <node <i>node-id</i> local primary>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display the hostname and version information about the software running on the device.
Options	<p>none—Display standard information about the hostname and version of the software running on the device.</p> <p>brief—Display brief output.</p> <p>detail—Display detailed output.</p> <p>node <i>node-id</i>—Display the software version on a specific node. Range: 0 through 1</p> <p>local—Display the software version on the local node.</p> <p>primary—Display the software version on the primary node.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Determining the Junos OS Version on page 138
List of Sample Output	show version on page 295

Sample Output

show version

```

user@host> show version
node0:
-----
Hostname: srx01
Model: srx1400
JUNOS Software Release [12.3I20141112_x_srx_12q3_x48_intgr.0-681573]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]

```


PART 3

CLI User Guide

- [Overview on page 299](#)
- [Getting Started: A Quick Tour of the CLI on page 309](#)
- [Getting Online Help on page 325](#)
- [Using Configuration Statements to Configure a Device on page 333](#)
- [Committing a Junos OS Configuration on page 371](#)
- [Managing Configurations on page 389](#)
- [Using Operational Commands to Monitor a Device on page 413](#)
- [Filtering Command Output on page 437](#)
- [Using Shortcuts, Wildcards, and Regular Expressions in the CLI on page 447](#)
- [Using Configuration Groups to Quickly Configure Devices on page 457](#)
- [Controlling the CLI Environment on page 483](#)
- [Junos OS Configuration Statements and Commands on page 489](#)
- [Junos OS CLI Environment Commands on page 521](#)
- [Junos OS CLI Operational Mode Commands on page 537](#)

CHAPTER 9

Overview

- [Introduction to Junos OS CLI on page 299](#)
- [Understanding the User Interfaces on page 301](#)
- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 304](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 307](#)
- [Commands and Configuration Statements for Junos-FIPS on page 307](#)

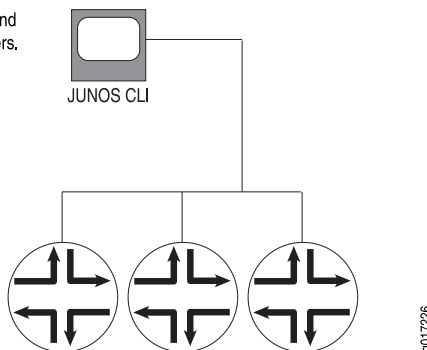
Introduction to Junos OS CLI

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 on page 299](#)). The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press Enter.

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 hierarchical 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 304](#)
- [Getting Started with the Junos OS Command-Line Interface on page 309](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 307](#)
- [Commands and Configuration Statements for Junos-FIPS on page 307](#)

Understanding the User Interfaces

You can use two user interfaces to configure, monitor, manage, and troubleshoot your device—the J-Web user interface and the command-line interface (CLI) for Junos OS.



NOTE: Other user interfaces facilitate the configuration of one or, in some cases, many devices on the network through a common API. Among the supported interfaces are the Junos Scope and Session and Resource Control (SRC) applications.

You can operate the device either in secure or router context. With the J-Web user interface and the CLI, you configure the routing protocols that run on the device and the device security features, including stateful firewall policies, Network Address Translation (NAT) attack prevention screens, Application Layer Gateways (ALGs), and IPsec VPNs. You also set the properties of its network interfaces. After activating a software configuration, you can use either user interface to monitor the system and the protocol traffic passing through the device, manage operations, and diagnose protocol and network connectivity problems.

This section contains the following topics:

- [J-Web User Interface on page 301](#)
- [CLI on page 303](#)

J-Web User Interface

The J-Web user interface allows you to monitor, configure, troubleshoot, and manage your device 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 device, so you can fully configure it without using the CLI editor.

You can perform the following tasks with the J-Web user interface:

- **Dashboard (SRX Series devices only)**—Views high-level details of Chassis View, system identification, resource utilization, security resources, system alarms, file usage, login sessions, chassis status, threats activity, and storage usage.
- **Configuring**—View the current configurations at a glance, configure the device, and manage configuration files. The J-Web user interface provides the following configuration methods:
 - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
 - Edit the configuration in a text file.
 - Upload a configuration file.
 - Use wizards to configure basic setup, firewall, VPN, and NAT settings on all SRX Series devices.

The J-Web user interface also allows you to manage configuration history and set a rescue configuration.

- **Monitoring**—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- **Managing**—Manage log, temporary, and core (crash) files and schedule reboots on your devices. You can also manage software packages and licenses, and copy a snapshot of the system software to a backup device.
- **Diagnosing**—Diagnose routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze control traffic on the devices.
- **Configuring and monitoring events**—Filter and view system log messages that record events occurring on the device. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.
- **Configuring and monitoring alarms**—Monitor and diagnose the device by monitoring active alarms that alert you to the conditions on a network interface. You can also set the conditions that trigger alarms on an interface.

[Table 37 on page 302](#) shows the maximum number of concurrent J-Web sessions on SRX Series devices.

Table 37: Concurrent J-Web Sessions on SRX Series Devices

Device Type	Maximum Number of Users
SRX100	3
SRX110	3
SRX210	3
SRX220	5
SRX240	5
SRX550	5
SRX650	5
SRX1400	1024
SRX3400	1024
SRX3600	1024
SRX5400	1024
SRX5600	1024

Table 37: Concurrent J-Web Sessions on SRX Series Devices (*continued*)

Device Type	Maximum Number of Users
SRX5800	1024

CLI

The CLI is a straightforward command-line interface in which you type commands on a line and press Enter to execute them. The CLI provides command Help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the device, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the device. This topic refers to configuration mode as the *CLI configuration editor*.

[Table 38 on page 303](#) shows the maximum number of concurrent CLI sessions on SRX Series devices.

Table 38: Concurrent CLI Sessions on SRX Series Devices

Device Type	Maximum Number of Users
SRX100	6
SRX110	6
SRX210	4
SRX220	9
SRX240	6
SRX550	11
SRX650	11
SRX1400	250
SRX3400	250
SRX3600	250
SRX5400	250
SRX5600	250

Table 38: Concurrent CLI Sessions on SRX Series Devices (*continued*)

Device Type	Maximum Number of Users
SRX5800	250

- Related Documentation**
- [Starting the J-Web User Interface on page 581](#)
 - [Understanding the J-Web Interface Layout on page 583](#)
 - [Getting Help in the J-Web User Interface on page 585](#)
 - [CLI User Guide](#)

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 304](#)
- [CLI Command Hierarchy on page 305](#)
- [Configuration Statement Hierarchy on page 305](#)
- [Moving Among Hierarchy Levels on page 306](#)

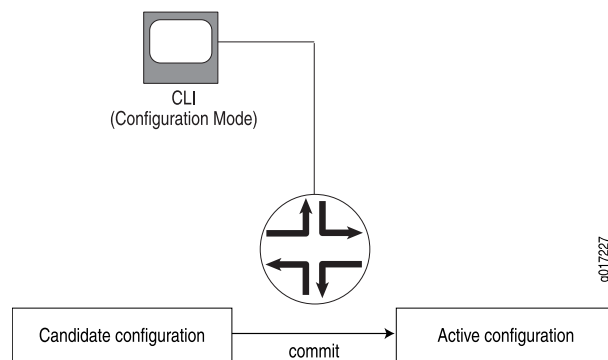
Junos OS CLI Command Modes

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 on page 305](#)). 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.

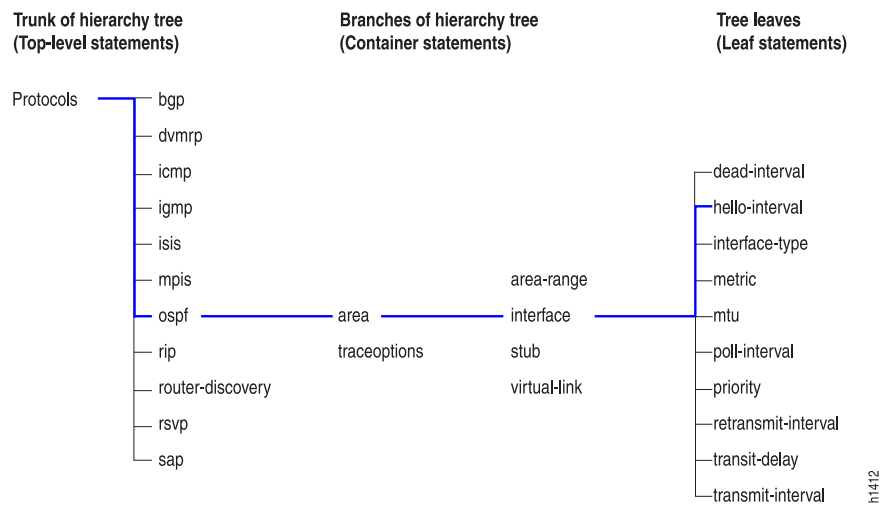
To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of the routes in the routing table, use the command **show route brief**.

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 on page 306 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 39 on page 306](#) to navigate the levels of the configuration statement hierarchy.

Table 39: 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

- [Introduction to Junos OS CLI on page 299](#)
- [Getting Started with the Junos OS Command-Line Interface on page 309](#)

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 *Configuration and Operations Automation 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 *SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices*.

Related Documentation

- [Introduction to Junos OS CLI on page 299](#)
- [Getting Started with the Junos OS Command-Line Interface on page 309](#)
- [Commands and Configuration Statements for Junos-FIPS on page 307](#)

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

- [Secure Configuration Guide for Common Criteria and Junos-FIPS](#).

Getting Started: A Quick Tour of the CLI

- [Getting Started with the Junos OS Command-Line Interface on page 309](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 311](#)
- [Configuring a User Account on a Device Running Junos OS on page 312](#)
- [Checking the Status of a Device Running Junos OS on page 314](#)
- [Example: Configuring a Routing Protocol on page 316](#)
- [Rolling Back Junos OS Configuration Changes on page 322](#)

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 325](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 311](#)
- [Checking the Status of a Device Running Junos OS on page 314](#)
- [Configuring a User Account on a Device Running Junos OS on page 312](#)
- [Example: Configuring a Routing Protocol on page 316](#)
- *Examples: Using the Junos OS CLI Command Completion*

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 304](#)
 - [Getting Online Help from the Junos OS Command-Line Interface on page 325](#)
 - [Configuring a User Account on a Device Running Junos OS on page 312](#)

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 309](#)
- [Getting Online Help from the Junos OS Command-Line Interface on page 325](#)
- [Displaying the Junos OS CLI Command and Word History on page 331](#)
- [Example: Configuring a Routing Protocol on page 316](#)

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 331](#)
- [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 429](#)
- [Viewing Files and Directories on a Device Running Junos OS on page 423](#)

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 317](#)
- [Longer Configuration on page 317](#)
- [Making Changes to a Routing Protocol Configuration on page 319](#)

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 re-create 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 309](#)
- [Displaying the Junos OS CLI Command and Word History on page 331](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 422](#)

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 Configuration on page 390](#)

CHAPTER 11

Getting Online Help

- [Getting Online Help from the Junos OS Command-Line Interface on page 325](#)
- [Junos OS CLI Online Help Features on page 327](#)
- [Examples: Using Command Completion in Configuration Mode on page 329](#)
- [Displaying the Junos OS CLI Command and Word History on page 331](#)

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 325](#)
- [Getting Help About a String in a Statement or Command on page 326](#)
- [Getting Help About Configuration Statements on page 327](#)
- [Getting Help About System Log Messages on page 327](#)

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.

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 feature guides. The **help reference** command displays summary information about the statement based on the summary descriptions that appear in the Junos OS feature 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 327](#)
 - [Getting Started with the Junos OS Command-Line Interface on page 309](#)

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 327](#)
- [Using CLI Command Completion on page 328](#)
- [Using Command Completion in Configuration Mode on page 328](#)
- [Displaying Tips About CLI Commands on page 328](#)

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 309](#)
 - *Examples: Using the Junos OS CLI Command Completion*

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](#)
 - [Displaying the Junos OS CLI Command and Word History on page 331](#)

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
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 327](#)

CHAPTER 12

Using Configuration Statements to Configure a Device

- [Understanding the Junos Configuration Groups on page 334](#)
- [Understanding Junos OS CLI Configuration Mode on page 335](#)
- [Entering and Exiting the Junos OS CLI Configuration Mode on page 341](#)
- [Forms of the configure Command on page 343](#)
- [Using the configure exclusive Command on page 344](#)
- [Example: Using the configure Command on page 345](#)
- [Modifying the Junos OS Configuration on page 346](#)
- [Adding Junos Configuration Statements and Identifiers on page 346](#)
- [Deleting a Statement from a Junos Configuration on page 348](#)
- [Example: Deleting a Statement from the Junos Configuration on page 349](#)
- [Copying a Junos Statement in the Configuration on page 350](#)
- [Example: Copying a Statement in the Junos Configuration on page 350](#)
- [Issuing Relative Junos Configuration Mode Commands on page 351](#)
- [Renaming an Identifier in a Junos Configuration on page 351](#)
- [Example: Renaming an Identifier in a Junos Configuration on page 352](#)
- [Inserting a New Identifier in a Junos Configuration on page 352](#)
- [Example: Inserting a New Identifier in a Junos Configuration on page 352](#)
- [Example: Using the Wildcard Command with the Range Option on page 354](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358](#)
- [Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 359](#)
- [Adding Comments in a Junos Configuration on page 360](#)
- [Example: Including Comments in a Junos Configuration on page 361](#)
- [Displaying the Current Junos OS Configuration on page 363](#)
- [Example: Displaying the Current Junos OS Configuration on page 364](#)
- [Displaying Additional Information About the Configuration on page 365](#)

- [Displaying set Commands from the Junos OS Configuration on page 367](#)
- [Displaying Users Currently Editing the Configuration on page 369](#)
- [Verifying a Junos Configuration on page 370](#)

Understanding the Junos Configuration Groups

This topic provides you an overview of the configuration groups feature and the inheritance model in Junos OS, and contains the following sections:

- [Configuration Groups Overview on page 334](#)
- [Inheritance Model on page 334](#)
- [Configuring Configuration Groups on page 335](#)

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 Junos OS command-line interface (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 need not 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 that the configuration statements contained in a configuration group are needed.

Related Documentation

- [Creating a Junos Configuration Group on page 457](#)

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 304, 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 336](#)
- [Configuration Statements and Identifiers on page 337](#)
- [Configuration Statement Hierarchy on page 339](#)

Configuration Mode Commands

Table 40 on page 336 summarizes each CLI configuration mode command. The commands are organized alphabetically.

Table 40: 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 40: 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 41 on page 338 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 41: 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>Administration Guide for Security Devices</i> .
accounting-options	Configure accounting statistics data collection for interfaces and firewall filters.
chassis	Configure properties of the router chassis, including conditions that activate alarms and SONET/SDH framing and concatenation properties.
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 Security Devices</i> .
firewall	Define filters that select packets based on their contents.
forwarding-options	Define forwarding options, including traffic sampling options.
groups	Configure configuration groups.
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>Interfaces Feature Guide for Security Devices</i> .
policy-options	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes.
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 Security Devices</i> and the <i>MPLS Feature Guide for Security Devices</i> .
routing-instances	Configure multiple routing instances. For information about the statements in this hierarchy, see the <i>Junos OS Routing Protocols Library for Security 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 Security Devices</i> .

Table 41: Configuration Mode Top-Level Statements (*continued*)

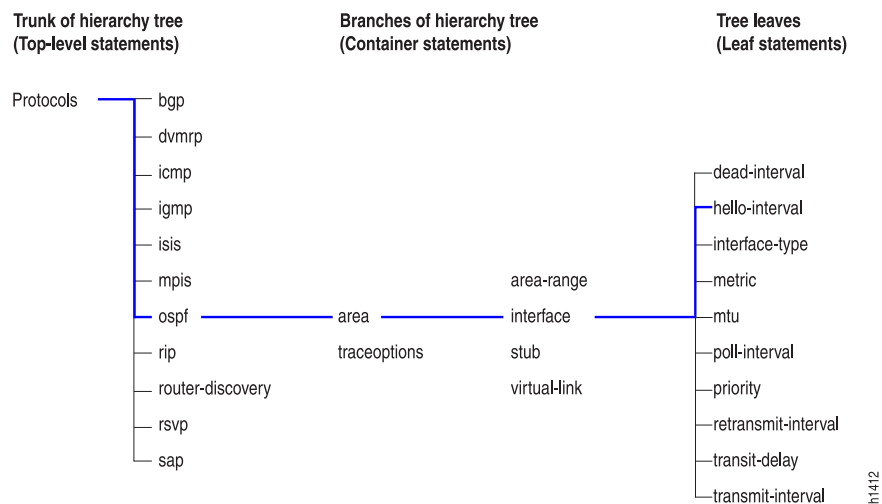
Statement	Description
security	Configure IP Security (IPsec) services.
snmp	Configure SNMP community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the <i>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices</i> .
system	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 specific information on configuration statements, see [CLI Explorer](#).

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 on page 339](#)). 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 on page 339](#) 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 on page 339](#) 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 341](#)

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 *Administration Guide for Security 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 335](#)
- [Modifying the Junos OS Configuration on page 346](#)
- [Commit Operation When Multiple Users Configure the Software on page 375](#)
- [Displaying the Current Junos OS Configuration on page 363](#)
- [Displaying set Commands from the Junos OS Configuration on page 367](#)
- [Issuing Relative Junos Configuration Mode Commands on page 351](#)
- [Using the configure exclusive Command on page 344](#)
- [Updating the configure private Configuration](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 311](#)

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 42 on page 343](#).

Table 42: 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. 	

Table 42: Forms of the configure Command (*continued*)

Command	Edit Access	Commit Access
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 372](#)
- [Example: Using the configure Command on page 345](#)
- [Displaying Users Currently Editing the Configuration on page 369](#)
- [Using the configure exclusive Command on page 344](#)
- [Updating the configure private Configuration](#)
- [Displaying set Commands from the Junos OS Configuration on page 367](#)

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 Configuration Statements and Identifiers on page 346](#)
 - [Forms of the configure Command on page 343](#)

Example: Using the configure Command

If, when you enter configuration mode, another user is also in configuration mode, a message shows who the user is and what part of the configuration that user 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#
```

If, when you enter configuration mode, the configuration contains changes that have not been committed, a message appears:

```
user@host> configure
Entering configuration mode
The configuration has been changed but not committed
[edit]
user@host#
```

- Related Documentation**
- [Forms of the configure Command on page 343](#)

Modifying the Junos OS Configuration

To configure a device running Junos OS or to modify an existing Junos 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 363](#)
- [Adding Junos Configuration Statements and Identifiers on page 346](#)
- [Using the configure exclusive Command on page 344](#)
- [Updating the configure private Configuration](#)
- [Issuing Relative Junos Configuration Mode Commands on page 351](#)

Adding Junos 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 346](#)
- [Deleting a Statement from a Junos Configuration on page 348](#)
- [Copying a Junos Statement in the Configuration on page 350](#)
- [Renaming an Identifier in a Junos Configuration on page 351](#)
- [Using the configure exclusive Command on page 344](#)
- [Additional Details About Specifying Junos Statements and Identifiers on page 395](#)
- [Displaying the Current Junos OS Configuration on page 363](#)

Deleting a Statement from a Junos Configuration

To delete a statement or identifier from a Junos 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 Configuration on page 349](#)
- [Adding Junos Configuration Statements and Identifiers on page 346](#)

- [Copying a Junos Statement in the Configuration on page 350](#)

Example: Deleting a Statement from the Junos 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 Configuration—Using the upto Option on page 454](#)
- [Deleting a Statement from a Junos Configuration on page 348](#)

Copying a Junos 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 350](#)
- [Adding Junos Configuration Statements and Identifiers on page 346](#)

Example: Copying a Statement in the Junos Configuration

The following example shows how you can create one virtual connection (VC) on an interface, and then copy its configuration to create a second VC:

```
[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;
    }
  }
}
[edit interfaces]
user@host# edit at-1/0/0
[edit interfaces at-1/0/0]
user@host# copy unit 61 to unit 62
[edit interfaces at-1/0/0]
```

```

user@host# show
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;
    }
}

```

Related Documentation • [Copying a Junos Statement in the Configuration on page 350](#)

Issuing Relative Junos 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 363](#)

Renaming an Identifier in a Junos 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 Configuration Statements and Identifiers on page 346](#)
 - [Example: Renaming an Identifier in a Junos Configuration on page 352](#)
 - [Inserting a New Identifier in a Junos Configuration on page 352](#)

Example: Renaming an Identifier in a Junos Configuration

This example shows how you can change the Network Time Protocol (NTP) server address to 10.0.0.6 using the **rename** configuration mode command:

```
[edit]
user@host# rename system network-time server 10.0.0.7 to server 10.0.0.6
```

- Related Documentation**
- [Renaming an Identifier in a Junos Configuration on page 351](#)

Inserting a New Identifier in a Junos 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 Configuration on page 351](#)
 - [Example: Renaming an Identifier in a Junos Configuration on page 352](#)
 - [Example: Inserting a New Identifier in a Junos Configuration on page 352](#)
 - [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358](#)

Example: Inserting a New Identifier in a Junos Configuration

Insert policy terms in a routing policy configuration. Note that if you do not use the **insert** command, but rather just configure another term, the added term is placed at the end

of the existing list of terms. Also note that you must create the term, as shown in this example, before you can place it with the **insert** command.

```
[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 reject;
    }
    term term4 {
      then accept;
    }
  }
}
[edit]
user@host# rename policy-options policy-statement statics 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
[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;  
}
```

Insert a transit router in a dynamic MPLS path:

```
[edit protocols mpls path ny-sf]  
user@host# show  
1.1.1.1;  
2.2.2.2;  
3.3.3.3 loose;  
4.4.4.4 strict;  
6.6.6.6;  
[edit protocols mpls path ny-sf]  
user@host# insert 5.5.5.5 before 6.6.6.6  
[edit protocols mpls path ny-sf]  
user@host# set 5.5.5.5 strict  
[edit protocols mpls path ny-sf]  
user@host# show  
1.1.1.1;  
2.2.2.2;  
3.3.3.3 loose;  
4.4.4.4 strict;  
5.5.5.5 strict;  
6.6.6.6;
```

- Related Documentation**
- [Inserting a New Identifier in a Junos Configuration on page 352](#)
 - [Adding Junos Configuration Statements and Identifiers on page 346](#)

Example: Using the Wildcard Command with the Range Option

- [Requirements on page 354](#)
- [Overview on page 355](#)
- [Configuration on page 355](#)
- [Verification on page 357](#)

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 356](#)
- [Specifying Multiple Ranges in the Syntax on page 356](#)
- [Specifying a Range and Unique Numbers In the Syntax on page 356](#)
- [Excluding Some Values from a Range on page 357](#)
- [Specifying a Range with a Step Number on page 357](#)

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 358](#)

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 356.

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 449

Deactivating and Reactivating Statements and Identifiers in a Junos 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.



NOTE: In Junos OS Release 10.3 and later, you can only deactivate identifiers or complete one-liner statements. You cannot deactivate just parts of a one-liner, such as only child or leaf statements. For example, in the following configuration:

```
[edit forwarding-options]
dhcp-relay {
    dynamic-profile dynamic-profile-name aggregate-clients;
}
```

You can deactivate the complete one-liner **dynamic profile *dynamic-profile-name* aggregate-clients**. However, you cannot deactivate *only* the **aggregate-clients** statement from the one-liner statement.

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 deactivate a statement, that specific object or property is completely ignored and is not applied at all when you issue a **commit** command. 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

- [Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 359](#)
- [Adding Junos Configuration Statements and Identifiers on page 346](#)

Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration

Deactivate an interface in the configuration:

```
[edit interfaces]
user@host# show
at-5/2/0 {
    traceoptions {
        traceflag all;
    }
    atm-options {
        vpi 0 maximum-vcs 256;
    }
    unit 0 {
        ...
    }
}
[edit interfaces]
user@host# deactivate at-5/2/0
[edit interfaces]
user@host# show
inactive: at-5/2/0 {
```

```

        traceoptions {
            traceflag all;
        }
        ...
    }
}

```

Reactivate the interface:

```

[edit interfaces]
user@host# activate at-5/2/0
[edit interfaces]
user@host# show
at-5/2/0 {
    traceoptions {
        traceflag all;
    }
    ...
}

```

Related Documentation

- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358](#)

Adding Comments in a Junos 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 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 ""
```

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.

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).

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.

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. .



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;
    }
  }
}
```

Related Documentation

- [Adding Junos Configuration Statements and Identifiers on page 346](#)
- [Example: Including Comments in a Junos Configuration on page 361](#)

Example: Including Comments in a Junos Configuration

To add comments to a Junos configuration:

```
[edit]
user@host# show
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0 {
```

```

        hello-interval 5;
    }
}
[edit]
user@host# edit protocols ospf
[edit protocols ospf]
user@host# set area 0.0.0.0
user@host# annotate area 0.0.0.0 "Backbone area configuration added June 15, 1998"
[edit protocols ospf]
user@host# edit area 0.0.0.0
[edit protocols ospf area 0.0.0.0]
user@host# annotate interface so0 "Interface from router sj1 to router sj2"
[edit protocols ospf area 0.0.0.0]
user@host# top
[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 {
        hello-interval 5;
      }
    }
  }
}
[edit]
user@host#

```

The following excerpt from a configuration example illustrates how to enter 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 */
}

```

**Related
Documentation**

- [Adding Comments in a Junos Configuration on page 360](#)

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'
    }
  }
}

```

**Related
Documentation**

- [Example: Displaying the Current Junos OS Configuration on page 364](#)
- [Displaying set Commands from the Junos OS Configuration on page 367](#)

Example: Displaying the Current Junos OS Configuration

The following example shows how you can display the current Junos configuration. To display the entire configuration:

```
[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;
      }
    }
  }
}
```

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;
}
```

Display all of the last committed 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
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 363](#)

Displaying Additional Information About the 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 367](#)

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 368](#)
- [Example: Displaying Required set Commands at the Current Hierarchy Level on page 368](#)
- [Example: Displaying set Commands with the match Option on page 369](#)

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 363](#)

Displaying Users Currently Editing the 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 Commit Operation” on page 377](#).

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 343](#)
 - [Using the configure exclusive Command on page 344](#)

Verifying a Junos 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 Configuration Statements and Identifiers on page 346](#)
 - [Committing a Junos OS Configuration on page 372](#)

Committing a Junos OS Configuration

- [Junos OS Commit Model for Router or Switch Configuration on page 371](#)
- [Committing a Junos OS Configuration on page 372](#)
- [Committing a Junos Configuration and Exiting Configuration Mode on page 375](#)
- [Commit Operation When Multiple Users Configure the Software on page 375](#)
- [Activating a Junos Configuration but Requiring Confirmation on page 376](#)
- [Scheduling a Junos Commit Operation on page 377](#)
- [Monitoring the Junos Commit Process on page 378](#)
- [Adding a Comment to Describe the Committed Configuration on page 379](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 380](#)
- [Junos OS Batch Commits Overview on page 380](#)
- [Example: Configuring Batch Commit Server Properties on page 381](#)

Junos OS Commit Model for Router or Switch Configuration

The router or switch configuration is saved using a commit model: that is, a candidate configuration is modified as desired and then committed to the system. Once a configuration has been 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 former active configuration file is saved as the first rollback configuration file (**juniper.conf.1.gz**), and all 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 (1–49) 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 **synchronization** command.

**Related
Documentation**

- *Configuring the Junos OS for the First Time on a Router or Switch with a Single Routing Engine*

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



NOTE: Do not use the load override or load replace command instead of set command in the management software Junos Space or NSM documentation.

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 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**

- [Committing a Junos Configuration and Exiting Configuration Mode on page 375](#)
- [Activating a Junos Configuration but Requiring Confirmation on page 376](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 380](#)
- [Forms of the configure Command on page 343](#)

Committing a Junos 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 Configuration but Requiring Confirmation on page 376](#)

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 372](#)
- [Forms of the configure Command on page 343](#)
- [Displaying Users Currently Editing the Configuration on page 369](#)

Activating a Junos 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.

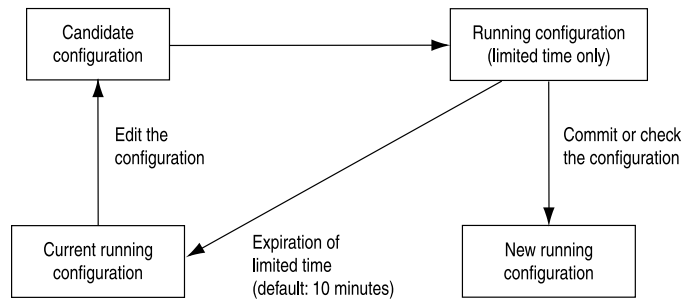
To show when a rollback is scheduled after a **commit confirmed** command, enter the **show system commit** command. For example:

```
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 on page 377 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 Commit Operation on page 377](#)
 - [Committing a Junos OS Configuration on page 372](#)

Scheduling a Junos 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 [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 372](#)
- [Monitoring the Junos Commit Process on page 378](#)

Monitoring the Junos 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 372](#)
- [Adding a Comment to Describe the Committed Configuration on page 379](#)

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 372](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 380](#)

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).

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 372](#)

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**.

Example: Configuring Batch Commit Server Properties

This example shows how to configure batch commit server properties to manage batch commit operations.

- [Requirements on page 381](#)
- [Overview on page 382](#)
- [Configuration on page 382](#)
- [Verification on page 384](#)

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 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 384](#)
- [Checking the Batch Commit Status on page 384](#)
- [Viewing the Patch Files in a Batch Commit Job on page 385](#)
- [Viewing the Trace Files for Batch Commit Operations on page 387](#)

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 380](#)
- [commit-interval \(Batch Commits\) on page 491](#)
- [days-to-keep-error-logs \(Batch Commits\) on page 491](#)
- [maximum-aggregate-pool \(Batch Commits\) on page 501](#)
- [maximum-entries \(Batch Commits\) on page 502](#)
- [maximum-entries on page 502](#)
- [server \(Batch Commits\) on page 510](#)
- [traceoptions \(Batch Commits\) on page 514](#)

Managing Configurations

- [Understanding How the Junos Configuration Is Stored on page 389](#)
- [Returning to the Most Recently Committed Junos Configuration on page 390](#)
- [Returning to a Previously Committed Junos OS Configuration on page 390](#)
- [Additional Details About Specifying Junos Statements and Identifiers on page 395](#)
- [Loading a Configuration from a File on page 398](#)
- [Examples: Loading a Configuration from a File on page 401](#)
- [Creating and Returning to a Rescue Configuration on page 403](#)
- [Example: Protecting the Junos OS Configuration from Modification or Deletion on page 404](#)
- [Synchronizing Routing Engines on page 410](#)

Understanding How the Junos 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.

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 switch's hard disk. 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

- [Returning to the Most Recently Committed Junos Configuration on page 390](#)
- [Returning to a Previously Committed Junos OS Configuration on page 390](#)
- [Loading a Configuration from a File on page 398](#)

Returning to the Most Recently Committed Junos 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 322](#)
- [Returning to a Previously Committed Junos OS Configuration on page 390](#)
- [Understanding How the Junos Configuration Is Stored on page 389](#)

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 390](#)
- [Displaying Previous Configurations on page 391](#)
- [Comparing Configuration Changes with a Prior Version on page 392](#)
- [Creating and Returning to a Rescue Configuration on page 393](#)
- [Saving a Configuration to a File on page 394](#)

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 33333;
    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, 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 [CLI Explorer](#).

Saving a Configuration to a File

Save the 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 Configuration on page 390](#)
- [Loading a Configuration from a File on page 398](#)
- [Specifying Filenames and URLs on page 426](#)

Additional Details About Specifying Junos 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 395](#)
- [Performing CLI Type-Checking on page 397](#)

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 43 on page 397](#) lists the data types the CLI checks.

Table 43: CLI Configuration Input Types

Data Type	Format	Examples
Physical interface name (used in the [edit interfaces] hierarchy)	<i>type-fpc/pic/port</i>	Correct: so-0/0/1 Incorrect: so-0
Full interface name	<i>type-fpc/pic/port<:channel>.logical</i>	Correct: so-0/0/1.0 Incorrect: so-0/0/1
Full or abbreviated interface name (used in places other than the [edit interfaces] hierarchy)	<i>type-<fpc</pic/port>><<:channel>.logical></i>	Correct: so, so-1, so-1/2/3:4.5

Table 43: CLI Configuration Input Types (*continued*)

Data Type	Format	Examples
IP address	<i>Oxhex-bytes</i> <i>octet</i> < <i>octet</i> < <i>octet</i> < <i>octet</i> >>>	<p>Correct: 1.2.3.4, 0x01020304, 128.8.1, 128.8</p> <p>Sample translations:</p> <p>1.2.3 becomes 1.2.3.0 0x01020304 becomes 1.2.3.4 0x010203 becomes 0.1.2.3</p>
IP address (destination prefix) and prefix length	<i>Oxhex-bytes</i> </ <i>length</i> > <i>octet</i> < <i>octet</i> < <i>octet</i> < <i>octet</i> >>></ <i>length</i> >	<p>Correct: 10/8, 128.8/16, 1.2.3.4/32, 1.2.3.4</p> <p>Sample translations:</p> <p>1.2.3 becomes 1.2.3.0/32 0x01020304 becomes 1.2.3.4/32 0x010203 becomes 0.1.2.3/32 default becomes 0.0.0.0/0</p>
International Organization for Standardization (ISO) address	<i>hex-nibble</i> < <i>hex-nibble ...</i> >	<p>Correct: 47.1234.2345.3456.00, 47.1234.2345.3456.00, 47.12.34.23.45.34.56.00</p> <p>Sample translations:</p> <p>47.123456 becomes 47.1234.56 47.12.34.56 becomes 47.1234.56 47.12.34.56 becomes 47.1234.56</p>
OSPF area identifier (ID)	<i>Oxhex-bytes</i> <i>octet</i> < <i>octet</i> < <i>octet</i> < <i>octet</i> >>> <i>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 0.0.1.1 128.8 becomes 128.8.0.0 0x010203 becomes 0.1.2.3</p>

Related Documentation • [Entering and Exiting the Junos OS CLI Configuration Mode on page 341](#)

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 426](#).

To load a configuration from the terminal, use the following version of the **load** configuration mode command. Type **^D** to end input.

```
[edit]
user@host# load (factory-default | merge | override | patch | replace | set | update)
terminal <relative>
```



NOTE: Do not use the **load override** or **load replace** command instead of **set** command in the management software Junos Space or NSM documentation.

To replace an entire configuration, specify the **override** option at any level of the hierarchy.

An override operation discards the current candidate configuration and loads the configuration in **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. For an example, see [Figure 15 on page 401](#).

To replace portions of a configuration, specify the **replace** option. 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 on page 401](#).

To replace only the configuration that has changed, specify the **update** option at any level of the hierarchy. An update operation compares the current configuration and the current candidate configuration, and loads only the changes between these configurations in **filename** or the one that you type at the terminal. When you use the update operation and commit the configuration, Junos OS attempts to notify the smallest set of system processes that are affected by the configuration change.

To combine the current configuration and the configuration in **filename** or the one that you type at the terminal, specify the **merge** option. A merge operation is useful when you are adding a new section to an existing configuration. If the existing configuration and the incoming configuration contain conflicting statements, the statements in the incoming configuration override those in the existing configuration. For an example, see [Figure 17 on page 401](#).

To change part of the configuration with a patch file and mark only those parts as changed, specify the **patch** option. For an example, see [Figure 18 on page 402](#).

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;

```

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.

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 on page 402](#).

To copy a configuration file from another network system to the local router, you can use the SSH and Telnet utilities.



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 401](#)

Examples: Loading a Configuration from a File

Figure 15: Overriding the Current Configuration

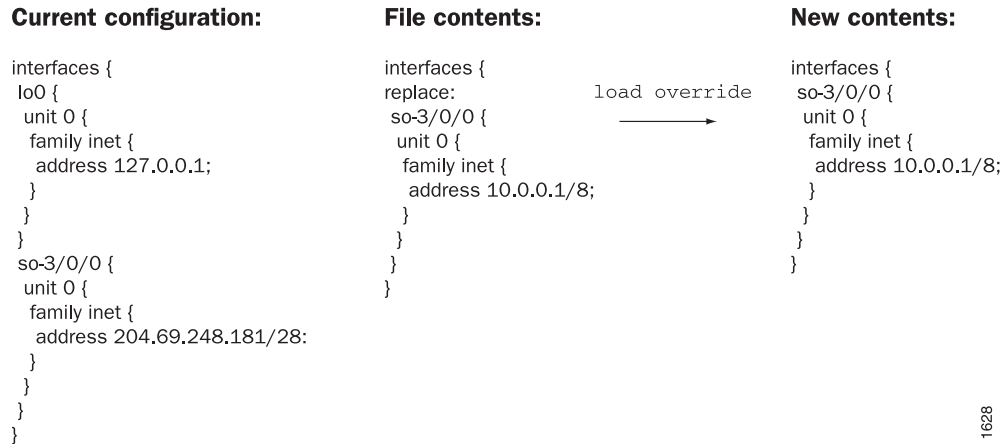


Figure 16: Using the replace Option

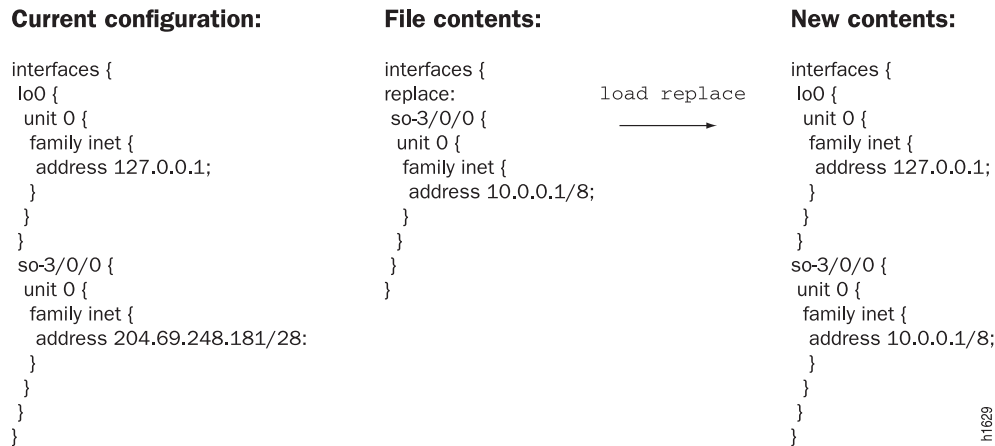


Figure 17: Using the merge Option

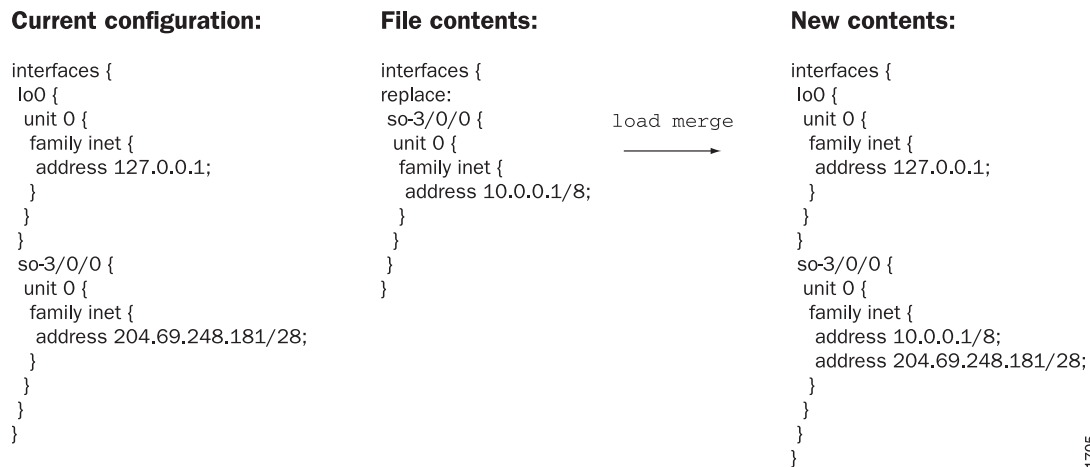


Figure 18: Using a Patch File**Current configuration:**

```

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 "$9$Ydg4ZDjqf5FVw"; ## SECRET-DATA
      }
    }
  }
}
}

```

g017215

Related Documentation

- [Loading a Configuration from a File on page 398](#)

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, 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 [CLI Explorer](#).

Related Documentation

- [Comparing Configuration Changes with a Prior Version on page 392](#)
- [Saving a Configuration to a File on page 394](#)

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 404](#)
- [Overview on page 404](#)
- [Protecting a Parent-Level Hierarchy on page 405](#)
- [Protecting a Child Hierarchy on page 405](#)
- [Protecting a Configuration Statement Within a Hierarchy on page 405](#)
- [Protecting a List of Identifiers for a Configuration Statement on page 406](#)
- [Protecting an Individual Member from a Homogenous List on page 406](#)
- [Unprotecting a Configuration on page 407](#)
- [Verification on page 407](#)

Requirements

This example uses the following hardware and software components:

- A M Series, MX 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];
}
```



**NOTE:** On SRX240 High Memory devices, when the **system login deny-sources** statement is used to restrict the access, it blocks a remote copy between nodes, which is used to copy the configuration during the commit routine. Use a firewall filter on the lo0.0 interface to restrict the Routing Engine access. However, if you choose to use the **system login deny-sources** statement, check the private addresses that were automatically on lo0.x and sp-0/0/0.x and exclude them from the denied list.

- 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 **protect="protect"** 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/11.2I0/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 Configuration Group” on page 459](#).

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, the 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 the Junos OS the First Time on a Router with Dual Routing Engines*

## CHAPTER 15

# Using Operational Commands to Monitor a Device

- [Overview of Junos OS CLI Operational Mode Commands on page 413](#)
- [Junos OS Operational Mode Commands That Combine Other Commands on page 416](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 417](#)
- [Controlling the Scope of an Operational Mode Command on page 418](#)
- [Monitoring Who Uses the Junos OS CLI on page 421](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 422](#)
- [Viewing Files and Directories on a Device Running Junos OS on page 423](#)
- [Displaying Junos OS Information on page 427](#)
- [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 429](#)
- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 434](#)
- [Example: Using Comments in Junos OS Operational Mode Commands on page 434](#)

## 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 413](#)
- [Commonly Used Operational Mode Commands on page 415](#)

### 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 304](#).
- 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 [CLI Explorer](#).
  - **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 [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 [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 [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 [CLI Explorer](#).
- A command—**start**—to exit the CLI and start a UNIX shell. For information about this command, see [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 335](#).
- A command—**quit**—to exit the CLI. For information about this command, see [CLI Explorer](#).

## Commonly Used Operational Mode Commands

Table 44 on page 415 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 44: Commonly Used Operational Mode Commands**

Items to Check	Description	Command
Software version	Versions of software running on the router or switch	<b>show version</b>
Log files	Contents of the log files	<b>monitor</b>
	Log files and their contents and recent user logins	<b>show log</b>
Remote systems	Host reachability and network connectivity	<b>ping</b>
	Route to a network system	<b>traceroute</b>
Configuration	Current system configuration	<b>show configuration</b>
Manipulate files	List of files and directories on the router or switch	<b>file list</b>
	Contents of a file	<b>file show</b>
Interface information	Detailed information about interfaces	<b>show interfaces</b>
Chassis	Chassis alarm status	<b>show chassis alarms</b>
	Information currently on craft display	<b>show chassis craft-interface</b>
	Router or switch environment information	<b>show chassis environment</b>
	Hardware inventory	<b>show chassis hardware</b>
Routing table information	Information about entries in the routing tables	<b>show route</b>
Forwarding table information	Information about data in the kernel's forwarding table	<b>show route forwarding-table</b>
IS-IS	Adjacent routers or switches	<b>show isis adjacency</b>
OSPF	Display standard information about OSPF neighbors	<b>show ospf neighbor</b>
BGP	Display information about BGP neighbors	<b>show bgp neighbor</b>

Table 44: Commonly Used Operational Mode Commands (*continued*)

Items to Check	Description	Command
MPLS	Status of interfaces on which MPLS is running	<b>show mpls interface</b>
	Configured LSPs on the router or switch, as well as all ingress, transit, and egress LSPs	<b>show mpls lsp</b>
	Routes that form a label-switched path	<b>show route label-switched-path</b>
RSVP	Status of interfaces on which RSVP is running	<b>show rsvp interface</b>
	Currently active RSVP sessions	<b>show rsvp session</b>
	RSVP packet and error counters	<b>show rsvp statistics</b>

**Related  
Documentation**

- [Junos OS Operational Mode Commands That Combine Other Commands on page 416](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 417](#)

## 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 on page 417](#).

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 413](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 417](#)

## 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 on page 418](#).)

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 413](#)
- [Controlling the Scope of an Operational Mode Command on page 418](#)

## 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 (or switch-fabric chassis)
- **lcc number**—A specific T640 router (in a routing matrix based on a TX Matrix router) or a TX Matrix Plus router (in a routing matrix based on a TX Matrix Plus router)
- **all-lcc**—All T640 routers (in a routing matrix based on a TX Matrix router) or all T1600 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: the TX Matrix router and all connected T640 routers or the TX Matrix Plus router and all connected T1600 routers.

## 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 422](#)
- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 434](#)

## 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 341](#)
  - [Controlling the Junos OS CLI Environment on page 483](#)

## 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 422](#)
- [Logical Part of an Interface Name on page 423](#)
- [Channel Identifier Part of an Interface Name on page 423](#)

### Physical Part of an Interface Name

The M Series Multiservices Edge Routers and the T Series Core Routers use one convention for interface naming, whereas the SRX Series Services Gateways use another.

- M Series and T Series interface names—On the M Series and T Series routers, 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.

- SRX Series interface names—On SRX Series 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*

For more information about SRX Series interface naming conventions, see the *Interfaces Feature Guide for Security Devices*.

## 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:

- M Series and T Series routers:

*type-fpc/pic/port.logical*

- SRX devices:

*type-slot/pim-or-ioc/port:channel.unit*

## 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 *Interfaces Feature Guide for Security Devices*.

A colon (:) separates the physical and virtual parts of the interface name:

- M Series and T Series routers:

*type-fpc/pic/port:channel*

*type-fpc//pic/port:channel:channel*

*type-fpc/pic/port:channel:channel:channel*

- 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*

### Related Documentation

- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 469](#)

## 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 424](#)
- [Listing Files and Directories on page 424](#)
- [Specifying Filenames and URLs on page 426](#)

## Directories on the Router or Switch

Table 45 on page 424 lists some standard directories on a device running Junos OS.

**Table 45: 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 ( <b>juniper.conf</b> ) 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 <b>traceoptions</b> 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.

1. 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 427](#)

## 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

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 429](#)

## 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 430](#)
- [Restarting a Junos OS Process on page 431](#)
- [Stopping the Junos OS on page 432](#)
- [Rebooting the Junos OS on page 433](#)

## 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 46 on page 431 lists and describes the output fields included in this example. The fields are listed in alphabetical order.

**Table 46: 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 ( <b>sleeping</b> , <b>running</b> , <b>starting</b> , <b>zombies</b> , and <b>stopped</b> ).
RES	Current amount of resident memory, in KB.
SIZE	Total size of the process ( <b>text</b> , <b>data</b> , and <b>stack</b> ), in KB.
STATE	Current state of the process ( <b>sleep</b> , <b>wait</b> , <b>run</b> , <b>idle</b> , <b>zombi</b> , or <b>stop</b> ).
Swap	Information about physical and virtual memory allocation.
USERNAME	Owner of the process.
WCPU	Weighted CPU usage.

## Restarting a 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 on page 432](#).)

Figure 22: Restarting a Process

	PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
PID before restart	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%	rpd
	553	root	2	0	8792K	1544K	select	0:01	0.00%	0.00%	mib2d
PID after 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%	rpd
	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%	vrrpd
	686	root	2	0	7808K	940K	select	0:00	0.00%	0.00%	apsd

## Stopping the 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 the Junos OS

After a software upgrade or to recover (occasionally) from an error condition, you must reboot Junos OS.

To reboot the 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 314](#)
  - [Displaying Junos OS Information on page 427](#)

---

## 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 434](#)

---

## 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 434](#)



# Filtering Command Output

- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 437](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 438](#)
- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 439](#)

## Using the Pipe ( | ) Symbol to Filter Junos 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 rip neighbor | ?
```

Possible completions:

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
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

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
```

#### Related Documentation

- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 439](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 438](#)

## Using Regular Expressions with the Pipe ( | ) Symbol to Filter Junos 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 47: 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 Command Output on page 437](#)
  - [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 439](#)

## 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 on page 439](#)
- [Counting the Number of Lines of Output on page 441](#)
- [Displaying Output in XML Tag Format on page 441](#)
- [Displaying the RPC tags for a Command on page 441](#)
- [Ignoring Output That Does Not Match a Regular Expression on page 441](#)
- [Displaying Output from the First Match of a Regular Expression on page 442](#)
- [Retaining Output After the Last Screen on page 442](#)
- [Displaying Output Beginning with the Last Entries on page 442](#)
- [Displaying Output That Matches a Regular Expression on page 443](#)
- [Preventing Output from Being Paginated on page 443](#)
- [Sending Command Output to Other Users on page 443](#)
- [Resolving IP Addresses on page 444](#)
- [Saving Output to a File on page 444](#)
- [Trimming Output by Specifying the Starting Column on page 444](#)

### Comparing Configurations

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. 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 nutmeg;
+ 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 {...}
```

## 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/tmp/</working-directory>
 </cli>
 <cli>
 <banner></banner>
 </cli>
</rpc-reply>
```

## 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 Command Output” on page 438](#).

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
sheep p0 baa.juniper.net 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 Command Output” on page 438](#).

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 Command Output” on page 438](#).

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>
```

## 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
```

**Related  
Documentation**

- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 438](#)
- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 437](#)



## CHAPTER 17

# Using Shortcuts, Wildcards, and Regular Expressions in the CLI

- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 447](#)
- [Using Wildcard Characters in Interface Names on page 449](#)
- [Common Regular Expressions to Use with the replace Command on page 450](#)
- [Using Global Replace in a Junos Configuration on page 451](#)
- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 452](#)
- [Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name on page 453](#)
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 454](#)
- [Using Regular Expressions to Delete Related Items from a Junos Configuration on page 455](#)

### 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 48 on page 448](#) lists some of the CLI keyboard sequences. They are the same as those used in Emacs.

Table 48: 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 48: 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 449](#)
  - [Using Global Replace in a Junos Configuration on page 451](#)

## 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 49 on page 449](#) lists the available wildcard characters. You must enclose all wildcard characters except the asterisk (\*) in quotation marks (" ").

Table 49: Wildcard Characters for Specifying Interface Names

Wildcard Character	Description
* (asterisk)	Match any string of characters in that position in the interface name. For example, <b>so*</b> 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, <b>so-"[03]"*</b> matches all SONET/SDH interfaces in slots 0 and 3.

Table 49: Wildcard Characters for Specifying Interface Names (*continued*)

Wildcard Character	Description
"[!character<character...>]"	Match all characters except the ones included in the brackets. For example, <b>so- "[!03]"</b> * matches all SONET/SDH interfaces except those in slots 0 and 3.
"[character1-character2]"	Match a range of characters. For example, <b>so- "[0-3]"</b> * 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, <b>so- "[!0-3]"</b> * 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 447](#)
  - [Using Global Replace in a Junos Configuration on page 451](#)

## Common Regular Expressions to Use with the replace Command

Table 50: 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 51 on page 451 lists some replacement examples.

**Table 51: 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&amp;def"</code>	Match: <code>1.1</code> Result: <code>abc1.1def</code>
<code>replace pattern 1.1 with "abc\&amp;def"</code>	Match: <code>1#1</code> Result: <code>abc&amp;def</code>

**Related Documentation**

- [Using Global Replace in a Junos Configuration on page 451](#)
- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 452](#)

## Using Global Replace in a Junos Configuration

You can make global changes to variables and identifiers in a Junos 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# replacepattern 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 450](#)
- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 452](#)
- [Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name on page 453](#)
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 454](#)
- [Using Wildcard Characters in Interface Names on page 449](#)
- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 447](#)

### Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference

The following example shows how you can use the **\n** back reference to replace a pattern:

```
[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;
 }
 }
}
[edit]
user@host# replace pattern "(.):1bf5" with "\11bf5"
[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;
 }
}

```

The pattern **2000::c0a8:1bf5** is replaced with **2000::c0a8:1bf5**.

- Related Documentation**
- [Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name on page 453](#)
  - [Using Global Replace in a Junos Configuration on page 451](#)

## Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name

The following example shows how you can replace an interface name in a configuration:

```

[edit]
user@host# show
protocols {
 ospf {
 area 0.0.0.0 {
 interface so-0/0/0 {
 hello-interval 5;
 }
 }
 }
}
[edit]
user@host# replace so-0/0/0 with so-1/1/0
[edit]
user@host# show
protocols {
 ospf {
 area 0.0.0.0 {
 interface so-1/1/0 {
 hello-interval 5;
 }
 }
 }
}

```

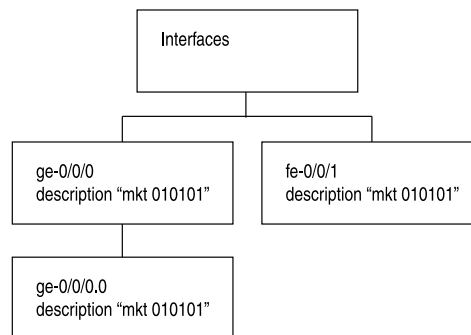
- Related Documentation**
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 454](#)
  - [Using Global Replace in a Junos Configuration on page 451](#)

## Example: Using Global Replace in a Junos Configuration—Using the upto Option

Consider the hierarchy shown in [Figure 23 on page 454](#). 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:

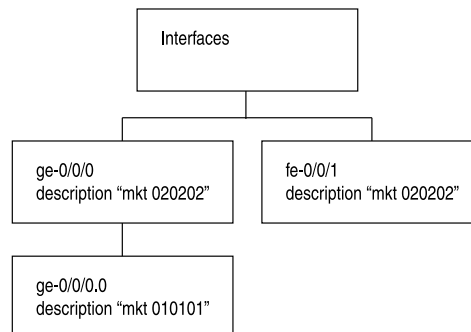
**Figure 23: Replacement by Object**

Current Configuration:



user@host > **replace pattern 01 with pattern 02 upto 2**

Resulting Configuration:



9017228

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 Configuration on page 451](#)

## Using Regular Expressions to Delete Related Items from a Junos Configuration

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 463](#)

## CHAPTER 18

# Using Configuration Groups to Quickly Configure Devices

- [Creating a Junos Configuration Group on page 457](#)
- [Applying a Junos Configuration Group on page 459](#)
- [Example: Configuring and Applying Junos Configuration Groups on page 460](#)
- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 462](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 463](#)
- [Using Wildcards with Configuration Groups on page 465](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 468](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 469](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 471](#)
- [Example: Configuring Peer Entities on page 472](#)
- [Establishing Regional Configurations on page 474](#)
- [Selecting Wildcard Names on page 475](#)
- [Example: Referencing the Preset Statement From the Junos defaults Group on page 477](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 478](#)
- [Using Conditions to Apply Configuration Groups Overview on page 478](#)
- [Example: Configuring Conditions for Applying Configuration Groups on page 478](#)
- [Using Junos OS Defaults Groups on page 481](#)

## Creating a Junos 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 481](#).

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 Configuration Group” on page 459](#).

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 Configuration Group on page 459](#)
- [Using Junos OS Defaults Groups on page 481](#)
- [Understanding the Junos Configuration Groups on page 334](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 463](#)
- [Using Wildcards with Configuration Groups on page 465](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 468](#)

## Applying a Junos Configuration Group

To have a Junos 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 Configuration Groups on page 460](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 463](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Using Wildcards with Configuration Groups on page 465](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 468](#)

---

## Example: Configuring and Applying Junos 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.



**NOTE:** Do not use the `load override` or `load replace` command instead of `set` command in the management software Junos Space or NSM documentation.

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 463.

#### Related Documentation

- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 462](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 469](#)
- [Example: Configuring Peer Entities on page 472](#)
- [Example: Referencing the Preset Statement From the Junos defaults Group on page 477](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 478](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 468](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 471](#)
- [Creating a Junos Configuration Group on page 457](#)

## 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 Configuration Groups on page 460](#)
- [Creating a Junos Configuration Group on page 457](#)

## 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 Configuration Group” on page 459](#).

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 Configuration Group on page 459](#)
- [Understanding the Junos Configuration Groups on page 334](#)

## 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

- [Selecting Wildcard Names on page 475](#)
- [Applying a Junos Configuration Group on page 459](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Understanding the Junos Configuration Groups on page 334](#)

## 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 the Junos Configuration Groups on page 334](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Applying a Junos Configuration Group on page 459](#)

## 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 the Junos Configuration Groups on page 334](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 422](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 471](#)

## 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 rel 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 Switches, is `em0`. Junos OS automatically creates the router's management Ethernet interface, `em0`.

#### Related Documentation

- [Understanding the Junos Configuration Groups on page 334](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 469](#)

## 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 the Junos Configuration Groups on page 334](#)
  - [Creating a Junos Configuration Group on page 457](#)
  - [Establishing Regional Configurations on page 474](#)

---

## 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 the Junos Configuration Groups on page 334](#)
  - [Example: Configuring Peer Entities on page 472](#)

## Selecting Wildcard Names

You can combine wildcarding and thoughtful use of names in statements to tailor statement values:

```

[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 465](#)

## Example: Referencing the Preset Statement From the Junos 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 478](#)
- [Using Junos OS Defaults Groups on page 481](#)
- [Understanding the Junos Configuration Groups on page 334](#)
- [Creating a Junos Configuration Group on page 457](#)

## 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 Configuration Group on page 457](#)
  - [Configuring Configuration Groups on page 335](#)

## 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 478](#)

## 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 478](#)
- [Overview on page 479](#)
- [Configuration on page 479](#)

### 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**, or **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. The configuration data has not yet been added to the **test1** group in this example.

## 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

The following example requires you to navigate various levels in the configuration hierarchy.

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.

**Results** From configuration mode, confirm your configuration by entering the **show groups** 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 480](#)

#### *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 the Junos Configuration Groups on page 334](#)
- [Creating a Junos Configuration Group on page 457](#)
- [Applying a Junos Configuration Group on page 459](#)
- [Using Conditions to Apply Configuration Groups Overview on page 478](#)

## 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 Configuration Group on page 457](#)
- [Example: Referencing the Preset Statement From the Junos defaults Group on page 477](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 478](#)



# Controlling the CLI Environment

- [Controlling the Junos OS CLI Environment on page 483](#)
- [Example: Controlling the CLI Environment on page 485](#)
- [Setting the Junos OS CLI Screen Length and Width on page 486](#)

## 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 484](#)
- [Setting the CLI Prompt on page 484](#)
- [Setting the CLI Directory on page 484](#)
- [Setting the CLI Timestamp on page 484](#)
- [Setting the Idle Timeout on page 484](#)

- [Setting the CLI to Prompt After a Software Upgrade on page 484](#)
- [Setting Command Completion on page 485](#)
- [Displaying CLI Settings on page 485](#)

## 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
```

### Related Documentation

- [Example: Controlling the CLI Environment on page 485](#)

## Example: Controlling the CLI Environment

The following example shows you how to change the default CLI environment:

```
user@host> set cli screen-length 66
Screen length set to 66
user@host> set cli screen-width 40
Screen width set to 40
user@host> set cli prompt "router1-san-jose > "
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 40
CLI terminal is 'xterm'
router1-san-jose >
```

### Related Documentation

- [Setting the Junos OS CLI Screen Length and Width on page 486](#)
- [Controlling the Junos OS CLI Environment on page 483](#)

## 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 486](#)
- [Setting the Screen Width on page 486](#)
- [Understanding the Screen Length and Width Settings on page 486](#)

### 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 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
```

### Understanding the Screen Length and Width Settings

The **cli screen-length** and **cli screen-width** settings in combination with each other and the size of the telnet or console window determine the extent of output displayed before each **--more--** prompt appears.

The following examples explain how the **cli screen-length** and **cli screen-width** values determine the appearance of the output:

- When the CLI screen width is set to the default value (80 characters) and the cli screen length to 10 lines, the **--more--** prompt appears on the tenth line of the output.
- When the CLI screen width is set to 20 characters and the CLI screen length is set to 6 lines in a telnet or console window that is wide enough to contain 40 characters, the **--more--** prompt appears on the fourth line of the output. Here each one of the first two lines has more than 20 characters and is counted as two lines. The third line contains the fifth line of output, and the fourth line contains the **--more--** prompt, which has to appear in the sixth line as per the setting.



**NOTE:** If you have inadvertently set the CLI screen width to a lower value that does not allow you to see the commands that you are typing, reset the CLI screen width with a higher value by entering the **set cli screen-width** command.

---



**TIP:** If you are not able to see the command that you are entering, type the command in a text editor and copy it at the command prompt.

**Related  
Documentation**

- [Example: Controlling the CLI Environment on page 485](#)
- [Controlling the Junos OS CLI Environment on page 483](#)



## CHAPTER 20

# Junos OS Configuration Statements and Commands

- [apply-groups on page 490](#)
- [apply-groups-except on page 490](#)
- [commit-interval \(Batch Commits\) on page 491](#)
- [days-to-keep-error-logs \(Batch Commits\) on page 491](#)
- [deactivate](#)
- [delete](#)
- [edit](#)
- [exit](#)
- [groups on page 496](#)
- [help](#)
- [insert](#)
- [load](#)
- [maximum-aggregate-pool \(Batch Commits\) on page 501](#)
- [maximum-entries \(Batch Commits\) on page 502](#)
- [protect](#)
- [quit](#)
- [rename](#)
- [replace](#)
- [rollback](#)
- [run](#)
- [save](#)
- [server \(Batch Commits\) on page 510](#)
- [set](#)
- [status](#)
- [top](#)
- [traceoptions \(Batch Commits\) on page 514](#)

- [unprotect](#)
- [up](#)
- [update](#)
- [when on page 518](#)
- [wildcard delete](#)

---

## apply-groups

---

<b>Syntax</b>	<code>apply-groups [ <i>group-names</i> ];</code>
<b>Hierarchy Level</b>	All hierarchy levels
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<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>
<b>Options</b>	<i>group-names</i> —One or more names specified in the <b>groups</b> statement.
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying a Junos Configuration Group on page 459</a></li><li>• <a href="#">groups on page 496</a></li></ul>

---

## apply-groups-except

---

<b>Syntax</b>	<code>apply-groups-except [ <i>group-names</i> ];</code>
<b>Hierarchy Level</b>	All hierarchy levels except the top level
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Disable inheritance of a configuration group.
<b>Options</b>	<i>group-names</i> —One or more names specified in the <b>groups</b> statement.
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">groups on page 496</a></li><li>• <a href="#">Disabling Inheritance of a Junos OS Configuration Group on page 463</a></li></ul>



## commit-interval (Batch Commits)

<b>Syntax</b>	<code>commit-interval <i>number-of-seconds-between-commits</i>;</code>
<b>Hierarchy Level</b>	[edit system commit server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	For Junos OS batch commits, specify the time interval (in seconds) between two commit operations.
<b>Options</b>	<p><i>number-of-seconds-between-commits</i>—Time interval (in seconds) between two commit operations.</p> <p><b>Range:</b> 1 through 30 seconds.</p> <p><b>Default:</b> 5 seconds.</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring Junos OS Batch Commits</i></li> </ul>

## days-to-keep-error-logs (Batch Commits)

<b>Syntax</b>	<code>days-to-keep-error-logs <i>days-to-keep-error-log-entries</i>;</code>
<b>Hierarchy Level</b>	[edit system commit server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	For Junos OS batch commits, specify the number of days to keep the error logs.
<b>Options</b>	<p><i>days-to-keep-error-log-entries</i>—Number of days to keep the error logs.</p> <p><b>Range:</b> 1 through 366 days</p> <p><b>Default:</b> 1 day</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring Junos OS Batch Commits</i></li> </ul>

## deactivate

---

<b>Syntax</b>	<code>deactivate (<i>statement</i>   <i>identifier</i>)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Add the <b>inactive:</b> 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 <b>commit</b> command.
<b>Options</b>	<p><b><i>identifier</i></b>—Identifier to which you are adding the <b>inactive:</b> tag. It must be an identifier at the current hierarchy level.</p> <p><b><i>statement</i></b>—Statement to which you are adding the <b>inactive:</b> tag. It must be a statement at the current hierarchy level.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">activate on page 538</a></li><li>• <a href="#">delete on page 493</a></li><li>• <a href="#">Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358.</a></li></ul>

---

## delete

---

<b>Syntax</b>	<code>delete &lt;statement-path&gt; &lt;identifier&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<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>
<b>Options</b>	<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>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">deactivate on page 492</a></li><li>• <a href="#">Deleting a Statement from a Junos Configuration on page 348</a></li></ul>

## edit

---

<b>Syntax</b>	<code>edit <i>statement-path</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Move inside the specified statement hierarchy. If the statement does not exist, it is created.</p> <p>You cannot use the <b>edit</b> command to change the value of identifiers. You must use the <b>set</b> command.</p>
<b>Options</b>	<i>statement-path</i> —Path to the statement.
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">set on page 511</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## exit

---

<b>Syntax</b>	exit <configuration-mode>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Exit the current level of the statement hierarchy, returning to the level prior to the last <b>edit</b> command, or exit from configuration mode. The <b>quit</b> and <b>exit</b> commands are synonyms.
<b>Options</b>	<p>none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.</p> <p><b>configuration-mode</b>—(Optional) Exit from configuration mode.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">top on page 513</a></li><li>• <a href="#">up on page 516</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## groups

```
Syntax groups {
 group-name {
 configuration-data;
 when {
 chassis chassis-id;
 member member-id;
 model model-id;
 node node-id;
 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 Switches, 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 Configuration Group on page 457](#)
  - [apply-groups on page 490](#)
  - [apply-groups-except on page 490](#)

## help

---

<b>Syntax</b>	<code>help &lt;(apropos <i>string</i>   reference &lt;<i>statement-name</i>&gt;   syslog &lt;<i>syslog-tag</i>&gt;   tip cli <i>number</i>   topic &lt;<i>word</i>&gt;)&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display help about available configuration statements or general information about getting help.
<b>Options</b>	<p><b>apropos <i>string</i></b>—(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><b>reference &lt;<i>statement-name</i>&gt;</b>—(Optional) Display summary information for the statement. This information is based on summary descriptions that appear in the Junos feature guides.</p> <p><b>syslog &lt;<i>syslog-tag</i>&gt;</b>—(Optional) Display information about system log messages.</p> <p><b>tip cli <i>number</i></b>—(Optional) Display a tip about using the CLI. Specify the number of the tip you want to view.</p> <p><b>topic &lt;<i>word</i>&gt;</b>—(Optional) Display usage guidelines for a topic or configuration statement. This information is based on subjects that appear in the Junos feature guides.</p> <p>Entering the <b>help</b> command without an option provides introductory information about how to use the <b>help</b> command.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Getting Online Help from the Junos OS Command-Line Interface on page 325</a></li></ul>



## insert

---

<b>Syntax</b>	<code>insert &lt;statement-path&gt; identifier1 (before   after) identifier2</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Insert an identifier in to an existing hierarchy.
<b>Options</b>	<p><b>after</b>—Place <i>identifier1</i> after <i>identifier2</i>.</p> <p><b>before</b>—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>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Inserting a New Identifier in a Junos Configuration on page 352</a></li></ul>

## load

---

<b>Syntax</b>	<code>load (factory-default   merge   override   patch   replace   set   update) load (<i>filename</i>   terminal) &lt;relative&gt;</code>
<b>QFX Series</b>	<code>load (dhcp-snooping <i>filename</i>)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	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.
<b>Options</b>	<p><b>dhcp-snooping</b>—(QFX Series switches) Loads DHCP snooping entries.</p> <p><b>factory-default</b>—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.</p> <p><b>filename</b>—Name of the file to load. For information about specifying the filename, see <a href="#">"Specifying Filenames and URLs" on page 426</a>.</p> <p><b>merge</b>—Combine the configuration that is currently shown in the CLI with the configuration.</p> <p><b>override</b>—Discard the entire configuration that is currently shown in the CLI and load the entire configuration. Marks every object as changed.</p> <p><b>patch</b>—Change part of the configuration and mark only those parts as changed.</p> <p><b>replace</b>—Look for a <b>replace</b> tag in <i>filename</i>, delete the existing statement of the same name, and replace it with the configuration.</p> <p><b>set</b>—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 <b>set</b>, <b>edit</b>, <b>exit</b>, and <b>top</b>.</p> <p><b>relative</b>—(Optional) Use the <b>merge</b> or <b>replace</b> option without specifying the full hierarchy level.</p> <p><b>terminal</b>—Use the text you type at the terminal as input to the configuration. Type Ctrl+d to end terminal input.</p> <p><b>update</b>—Discard the entire configuration that is currently shown in the CLI, and load the entire configuration. Marks changed objects only.</p>



**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](#).



**NOTE:** Do not use the `load override` or `load replace` command instead of the `set` command in the management software Junos Space or NSM documentation.

<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Loading a Configuration from a File on page 398</a></li> </ul>

## maximum-aggregate-pool (Batch Commits)

<b>Syntax</b>	<code>maximum-aggregate-pool <i>maximum-number-of-commits-to-aggregate</i>;</code>
<b>Hierarchy Level</b>	[edit system commit server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	For Junos OS batch commits, specify the maximum number of individual commit operations that are aggregated or merged into a single commit operation.
<b>Options</b>	<p><b><i>maximum-number-of-commits-to-aggregate</i></b>—Maximum number of individual commit operations that are aggregated or merged into a single commit operation.</p> <p><b>Range:</b> 1 through 4294967295</p> <p><b>Default:</b> 5</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Junos OS Batch Commits</a></li> </ul>

## maximum-entries (Batch Commits)

---

<b>Syntax</b>	<code>maximum-entries <i>number-of-entries</i>;</code>
<b>Hierarchy Level</b>	[edit system commit server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	For Junos OS batch commits, specify the maximum number of commit jobs that are included in the commit queue.
<b>Options</b>	<i>number-of-entries</i> —Maximum number of commit jobs that are included in the commit queue.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Example: Configuring Junos OS Batch Commits</i></li></ul>

## protect

---

<b>Syntax</b>	<code>protect (<i>hierarchy</i>   <i>statement</i>   <i>identifier</i>)</code>
<b>Release Information</b>	Command introduced in Junos OS Release 11.2.
<b>Description</b>	Protect a hierarchy, statement, or identifier from modification or deletion.
<b>Options</b>	none
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Protecting the Junos OS Configuration from Modification or Deletion on page 404</a></li></ul>

## quit

---

<b>Syntax</b>	quit <configuration-mode>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Exit the current level of the statement hierarchy, returning to the level prior to the last <b>edit</b> command, or exit from configuration mode. The <b>quit</b> and <b>exit</b> commands are synonyms.
<b>Options</b>	<p>none—Return to the previous edit level. If you are at the top of the statement hierarchy, exit configuration mode.</p> <p><b>configuration-mode</b>—(Optional) Exit from configuration mode.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">top on page 513</a></li><li>• <a href="#">up on page 516</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## 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 Configuration on page 351](#)

## replace

---

<b>Syntax</b>	replace pattern <i>pattern1</i> with <i>pattern2</i> <upto <i>n</i> >
<b>Release Information</b>	Command introduced in Junos OS Release 7.6.
<b>Description</b>	Replace identifiers or values in a configuration.
<b>Options</b>	<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><b>upto <i>n</i></b>—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 <b>upto</b> option, all identifiers and values in the configuration that match <i>pattern1</i> are replaced.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Using Global Replace in a Junos Configuration on page 451</a></li></ul>



## rollback

<b>Syntax</b>	<code>rollback &lt;number   rescue&gt;</code>
<b>Release Information</b>	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	<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 <b>commit</b> configuration command.</p> <p>The currently operational Junos OS configuration is stored in the file <b>juniper.conf</b>, and the last three committed configurations are stored in the files <b>juniper.conf.1</b>, <b>juniper.conf.2</b>, and <b>juniper.conf.3</b>. These four files are located in the directory <b>/config</b>, which is on the router's flash drive. The remaining 46 previous committed configurations, the files <b>juniper.conf.4</b> through <b>juniper.conf.49</b>, are stored in the directory <b>/var/db/config</b>, 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 <b>load update</b>).</p>
<b>Options</b>	<p><b>none</b> (Optional)—Return to the most recently saved configuration.</p> <p><b>number</b>—(Optional) Configuration to return to. The range of values is from <b>0</b> through <b>49</b>. The most recently saved configuration is number <b>0</b>, and the oldest saved configuration is number <b>49</b>. The default is <b>0</b>.</p> <p><b>rescue</b>—(Optional) Return to the rescue configuration.</p>
<b>Required Privilege Level</b>	rollback—To roll back to configurations other than the one most recently committed.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Returning to a Previously Committed Junos OS Configuration on page 390</a></li> <li>• <a href="#">Creating and Returning to a Rescue Configuration on page 393</a></li> </ul>

## run

---

<b>Syntax</b>	<code>run <i>command</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Run a top-level CLI command without exiting from configuration mode.
<b>Options</b>	<i>command</i> —CLI top-level command.
<b>Required Privilege Level</b>	configure—To enter configuration mode.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Junos OS CLI Configuration Mode on page 335</a></li></ul>

## save

<b>Syntax</b>	<code>save <i>filename</i></code>
<b>QFX Series</b>	<code>save (dhcp-snooping <i>filename</i>)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	<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 <b>scp/ssh</b> protocol.</p>
<b>Options</b>	<p><b><i>filename</i></b>—Name of the saved file. You can specify a filename in one of the following ways:</p> <ul style="list-style-type: none"> <li>• <b><i>filename</i></b>—File in the user's home directory (the current directory) on the local flash drive.</li> <li>• <b><i>path/filename</i></b>—File on the local flash drive.</li> <li>• <b><i>/var/filename</i></b> or <b><i>/var/path/filename</i></b>—File on the local hard disk.</li> <li>• <b><i>a:filename</i></b> or <b><i>a:path/filename</i></b>—File on the local drive. The default path is <b>/</b> (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.</li> <li>• <b><i>hostname:/path/filename</i></b>, <b><i>hostname:filename</i></b>, <b><i>hostname:path/filename</i></b>, or <b><i>scp://hostname/path/filename</i></b>—File on an <b>scp/ssh</b> 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 <b><i>hostname</i></b> as <b><i>username@hostname</i></b>.</li> <li>• <b><i>ftp://hostname/path/filename</i></b>—File on an FTP server. You can also specify <b><i>hostname</i></b> as <b><i>username @hostname</i></b> or <b><i>username:password @hostname</i></b>. The default path is the user's home directory. To specify an absolute path, the path must start with the string <b>%2F</b>; for example, <b><i>ftp://hostname/%2Fpath/filename</i></b>. To have the system prompt you for the password, specify <b><i>prompt</i></b> in place of the password. If a password is required, and you do not specify the password or <b><i>prompt</i></b>, an error message is displayed:           <pre>user@host&gt; file copy ftp://username@ftp.hostname.net//filename file copy ftp.hostname.net: Not logged in. user@host&gt; file copy ftp://username:prompt@ftphostname.net//filename</pre> <p>Password for <b><i>username@ftp.hostname.net</i></b>:</p> </li> <li>• <b><i>http://hostname/path/filename</i></b>—File on a Hypertext Transfer Protocol (HTTP) server. You can also specify <b><i>hostname</i></b> as <b><i>username@hostname</i></b> or <b><i>username:password@hostname</i></b>. If a password is required and you omit it, you are prompted for it.</li> <li>• <b><i>re0:/path/filename</i></b> or <b><i>re1:/path/filename</i></b>—File on a local Routing Engine.</li> </ul>

**Required Privilege Level** configure—To enter configuration mode.

**Related Documentation**

- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358](#)

---

## 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** For Junos OS batch commits, configure the batch commit server properties.  
  
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**

- *Example: Configuring Junos OS Batch Commits*

## set

---

<b>Syntax</b>	<code>set &lt;<i>statement-path</i>&gt; <i>identifier</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Create a statement hierarchy and set identifier values. This is similar to <b>edit</b> except that your current level in the hierarchy does not change.
<b>Options</b>	<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>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">edit on page 494</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## status

---

<b>Syntax</b>	status
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display the users currently editing the configuration.
<b>Required Privilege Level</b>	configure—To enter configuration mode. <ul style="list-style-type: none"><li>• <a href="#">“Displaying Users Currently Editing the Configuration” on page 369.</a></li></ul>

## top

---

<b>Syntax</b>	<code>top &lt;configuration-command&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Return to the top level of configuration command mode, which is indicated by the <b>[edit]</b> banner.
<b>Options</b>	<i>configuration-command</i> —(Optional) Issue configuration mode commands from the top of the hierarchy.
<b>Required Privilege Level</b>	configure—To enter configuration mode.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li><li>• <a href="#">exit on page 495</a></li><li>• <a href="#">up on page 516</a></li></ul>

## tracoptions (Batch Commits)

<b>Syntax</b>	<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>
<b>Hierarchy Level</b>	[edit system commit server]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	For Junos OS batch commits, configure tracing operations.
<b>Options</b>	<b>file <i>name</i></b> —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.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring Junos OS Batch Commits</i></li> </ul>



## unprotect

---

<b>Syntax</b>	<code>unprotect (<i>hierarchy</i>   <i>statement</i>   <i>identifier</i>)</code>
<b>Release Information</b>	Command introduced in Junos OS Release 11.2.
<b>Description</b>	Unprotect a protected hierarchy, configuration statement, or an identifier.
<b>Options</b>	none
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">top on page 513</a></li><li>• <a href="#">up on page 516</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## up

---

<b>Syntax</b>	<code>up &lt;number&gt; &lt;configuration-command&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Move up one level in the statement hierarchy.
<b>Options</b>	<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>
<b>Required Privilege Level</b>	configure—To enter configuration mode.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li><li>• <a href="#">exit on page 495</a></li><li>• <a href="#">top on page 513</a></li></ul>

## 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.*

## when

<b>Syntax</b>	<pre> when {   chassis <i>chassis-id</i>;   member <i>member-id</i>;   model <i>model-id</i>;   node <i>node-id</i>;   routing-engine <i>routing-engine-id</i>;   time &lt;<i>start-time</i>&gt; [to &lt;<i>end-time</i>&gt;]; } </pre>
<b>Hierarchy Level</b>	[edit groups <i>group-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.3.
<b>Description</b>	<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>
<b>Options</b>	<p><b>chassis</b> <i>chassis-id</i>—Specify the chassis type of the router. Valid types include SCC0, SCC1, LCC0, LCC1 ... LCC3.</p> <p><b>member</b> <i>member-id</i>—Specify the name of the member of the virtual chassis.</p> <p><b>model</b> <i>model-id</i>—Specify the model name of the router, such as m7i or tx100.</p> <p><b>node</b> <i>node-id</i>—Specify the cluster node.</p> <p><b>routing-engine</b> <i>routing-engine-id</i>—Specify the type of Routing Engine, re0 or re1.</p> <p><b>time</b> &lt;<i>start-time</i>&gt; [to &lt;<i>end-time</i>&gt;]—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: <b>time</b> &lt;<i>start-time</i>&gt; [to &lt;<i>end-time</i>&gt;] using the time format yyyy-mm-dd.hh:mm, hh:mm, or hh.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Creating a Junos Configuration Group on page 457</a></li> <li>• <a href="#">apply-groups on page 490</a></li> <li>• <a href="#">apply-groups-except on page 490</a></li> <li>• <a href="#">groups on page 496</a></li> </ul>

## wildcard delete

---

<b>Syntax</b>	<code>wildcard delete &lt;statement-path&gt; &lt;identifier&gt; &lt;regular-expression&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<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>
<b>Options</b>	<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 <b>wildcard</b> 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>
<b>Required Privilege Level</b>	configure—To enter configuration mode. Other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 454.</a></li></ul>



## CHAPTER 21

# 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 authorization`
- `show cli directory`
- `show cli history`

## set cli complete-on-space

---

<b>Syntax</b>	set cli complete-on-space (off   on)
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	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.
<b>Options</b>	<b>off</b> —Turn off command completion. <b>on</b> —Allow either a space or a tab to be used for command completion.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show cli on page 532</a></li></ul>
<b>List of Sample Output</b>	<a href="#">set cli complete-on-space on page 522</a>
<b>Output Fields</b>	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

---

<b>Syntax</b>	set cli directory <i>directory</i>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Set the current working directory.
<b>Options</b>	<i>directory</i> —Pathname of the working directory.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">set cli directory on page 523</a>
<b>Output Fields</b>	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

---

<b>Syntax</b>	set cli idle-timeout < <i>minutes</i> >
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Set the maximum time that an individual session can be idle before the user is logged off the router or switch.
<b>Options</b>	<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.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">set cli idle-timeout on page 524</a>
<b>Output Fields</b>	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

---

<b>Syntax</b>	set cli prompt <i>string</i>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Set the prompt so that it is displayed within the CLI.</p> <pre>user@host&gt; set cli prompt lab1-router&gt;</pre>
<b>Options</b>	<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> .
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the CLI Prompt on page 484</a></li></ul>

## set cli restart-on-upgrade

---

<b>Syntax</b>	set cli restart-on-upgrade string (off   on)
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For an individual session, set the CLI to prompt you to restart the router after upgrading the software.</p> <pre>user@host&gt; set cli restart-on-upgrade on Enabling restart-on-upgrade</pre>
<b>Options</b>	<p><b>off</b>—Disables the prompt.</p> <p><b>on</b>—Enables the prompt.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the CLI to Prompt After a Software Upgrade on page 484</a></li></ul>

---

## set cli screen-length

---

<b>Syntax</b>	set cli screen-length <i>length</i>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Set terminal screen length.</p> <pre>user@host&gt; set cli screen-length 75 Screen Length set to 75</pre>
<b>Options</b>	<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 ---(<b>more</b>)--- prompt appears on the screen is a function of this setting and the settings for the <b>set cli screen-width</b> and <b>set cli terminal</b> commands.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the Screen Length on page 486</a></li><li>• <a href="#">Understanding the Screen Length and Width Settings on page 486</a></li><li>• <a href="#">set cli screen-width on page 528</a></li><li>• <a href="#">set cli terminal on page 529</a></li><li>• <a href="#">show cli</a></li></ul>

## set cli screen-width

---

<b>Syntax</b>	set cli screen-width <width>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Set the terminal screen width.</p> <pre>user@host&gt; set cli screen-width 132 Screen width set to 132</pre>
<b>Options</b>	<p><b>width</b>—Number of characters in a line. The value is 0 or in the range of 0 through 1024. The default value is 80.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the Screen Width on page 486</a></li><li>• <a href="#">set cli screen-length on page 527</a></li><li>• <a href="#">set cli terminal on page 529</a></li><li>• <a href="#">show cli</a></li></ul>

---

## set cli terminal

---

<b>Syntax</b>	set cli terminal <i>terminal-type</i>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Set the terminal type.</p> <pre>user@host&gt; set cli terminal xterm</pre>
<b>Options</b>	<p><i>terminal-type</i>—Type of terminal that is connected to the Ethernet management port:</p> <ul style="list-style-type: none"><li>• <b>ansi</b>—ANSI-compatible terminal (80 characters by 24 lines)</li><li>• <b>small-xterm</b>—Small xterm window (80 characters by 24 lines)</li><li>• <b>vt100</b>—VT100-compatible terminal (80 characters by 24 lines)</li><li>• <b>xterm</b>—Large xterm window (80 characters by 65 lines)</li></ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the Terminal Type on page 484</a></li></ul>

## set cli timestamp

---

<b>Syntax</b>	set cli timestamp (format <i>timestamp-format</i>   disable)
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Set a timestamp for CLI output.</p> <pre>user@host&gt; set cli timestamp format '%m-%d-%T' '04-21-17:39:13' CLI timestamp set to: '%m-%d-%T'</pre>
<b>Options</b>	<p><b>format <i>timestamp-format</i></b>—Set the data 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"><li>• <b>%m</b>—Two-digit month</li><li>• <b>%d</b>—Two-digit date</li><li>• <b>%T</b>—Six-digit hour, minute, and seconds</li></ul> <p>Enclose the format in single quotation marks ( ' ). Do not use spaces. Use a hyphen ( - ) or similar character to separate placeholders.</p> <p><b>disable</b>—Remove the timestamp from the CLI.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Setting the CLI Timestamp on page 484</a></li></ul>



---

## set date

---

**Syntax**    `set date (date-time | ntp <ntp-server> <source-address source-address>)`

**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**
- ***date-time***—Specify date and time in one of the following formats:
    - *YYYYMMDDHHMM.SS*
    - “*month DD, YYYY HH:MM(am | pm)*”
  - **ntp**—Configure the router to synchronize the current date and time setting with a Network Time Protocol (NTP) server.
  - ***ntp-server***—(Optional) Specify the IP address of one or more NTP servers.
  - ***source-address source-address***—(Optional) Specify the source address that is used by the router to contact the remote NTP server.

**Required Privilege Level**    view

## show cli

<b>Syntax</b>	show cli
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display configured CLI settings.
<b>Options</b>	This command has no options.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show cli on page 532</a>
<b>Output Fields</b>	<a href="#">Table 52 on page 532</a> lists the output fields for the <b>show cli</b> command. Output fields are listed in the approximate order in which they appear.

**Table 52: 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: <b>on</b> or <b>off</b> .
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 <b>disabled</b> .
CLI restart-on-upgrade	CLI is set to prompt you to restart the router or switch after upgrading the software: <b>on</b> or <b>off</b> .
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: <b>enhanced</b> .
CLI timestamp	Date and time format for the timestamp. If the timestamp is not set, the state is <b>disabled</b> .
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 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

---

<b>Syntax</b>	show cli directory
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display the current working directory.  user@host> <b>show cli directory</b> Current directory: /var/tmp
<b>Required Privilege Level</b>	view

## show cli history

---

<b>Syntax</b>	<code>show cli history &lt;count&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Display a list of previous CLI commands.</p> <pre>user@host&gt; show cli history 11:14:14 -- show arp 11:22:10 -- show cli authorization 11:27:12 -- show cli history</pre>
<b>Options</b>	<p>none—Display all previous CLI commands.</p> <p><i>count</i>—(Optional) Maximum number of commands to display.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Displaying the Junos OS CLI Command and Word History on page 331</a></li></ul>

## CHAPTER 22

# Junos OS CLI Operational Mode Commands

- activate
- annotate
- commit
- configure
- copy
- file
- help
- | (pipe)
- request
- restart
- set
- show
- show configuration
- show | display inheritance
- show | display omit
- show | display set
- show | display set relative
- show groups junos-defaults
- show system commit

## activate

---

<b>Syntax</b>	<code>activate (<i>statement</i>   <i>identifier</i>)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Remove the <b>inactive:</b> 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 <b>commit</b> command.
<b>Options</b>	<p><b><i>identifier</i></b>—Identifier from which you are removing the <b>inactive</b> tag. It must be an identifier at the current hierarchy level.</p> <p><b><i>statement</i></b>—Statement from which you are removing the <b>inactive</b> tag. It must be a statement at the current hierarchy level.</p>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">deactivate on page 492</a></li><li>• <a href="#">Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358</a></li></ul>



## 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 onliners. However, annotation of parts (child statements or identifiers within a onliner) of the onliner is not supported. For example, in the following sample configuration hierarchy, annotation is supported up to the onliner 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 Configuration on page 360](#)

## commit

**Syntax** `commit <<at <"string">> <and-quit> <check> <comment <"comment-string">>  
<confirmed> <display detail> <minutes> <synchronize><force>>`

**Release Information** Command introduced before Junos OS Release 7.4.

**Description** Commit the set of changes to the database and cause the changes to take operational effect.

**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 [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.

**synchronize** <*force*>—(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 (request 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 is terminated and its configuration synchronized with that on the Routing Engine from which you issued the command.



**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 463](#).

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](#).



**NOTE:** Do not use the `load override` or `load replace` command instead of `set` command in the management software Junos Space or NSM documentation.

**Related Documentation**

- [Verifying a Junos Configuration on page 370](#), [Committing a Junos OS Configuration on page 372](#)
- [Scheduling a Junos Commit Operation on page 377](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 358](#)
- [Monitoring the Junos Commit Process on page 378](#)
- [Adding a Comment to Describe the Committed Configuration on page 379](#)

## configure

<b>Syntax</b>	configure <batch> <dynamic> <exclusive> <private>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	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.
<b>Options</b>	<p><b>none</b>—Enter configuration mode.</p> <p><b>batch</b>—(Optional) Work in the batch commit mode where commit operations are executed in batches.</p> <p><b>dynamic</b>—(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><b>exclusive</b>—(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><b>private</b>—(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>
<b>Required Privilege Level</b>	configure
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show configuration on page 564</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">configure on page 544</a>
<b>Output Fields</b>	When you enter this command, you are placed in configuration mode and the system prompt changes from <i>hostname&gt;</i> to <i>hostname#</i> .

## Sample Output

### configure

```
user@host> configure
Entering configuration mode
[edit]
user@host#
```

## copy

---

<b>Syntax</b>	<code>copy <i>existing-statement</i> to <i>new-statement</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Make a copy of an existing statement in the configuration.
<b>Options</b>	<i>existing-statement</i> —Statement to copy. <i>new-statement</i> —Copy of the statement.
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Copying a Junos Statement in the Configuration on page 350</a></li></ul>

## file

---

<b>Syntax</b>	<code>file &lt;archive   checksum   compare   copy   delete   list   rename   show   source address   archive&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	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.
<b>Options</b>	<p><b>archive (Optional)</b>—Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.</p> <p><b>checksum (Optional)</b>—Calculate the Message Digest 5 (MD5) checksum of a file.</p> <p><b>compare (Optional)</b>—Compare two local files and describe the differences between them in default, context, or unified output styles.</p> <p><b>copy (Optional)</b>—Copy files from one place to another on the local switch or between the local switch and a remote system.</p> <p><b>delete (Optional)</b>—Delete a file on the local switch.</p> <p><b>list (Optional)</b>—Display a list of files on the local switch.</p> <p><b>rename (Optional)</b>—Rename a file on the local switch.</p> <p><b>show (Optional)</b>—Display the contents of a file.</p> <p><b>source address (Optional)</b>—Specify the source address of the local file.</p>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Viewing Files and Directories on a Device Running Junos OS on page 423</a></li></ul>



## help

---

<b>Syntax</b>	<code>help &lt; (apropos <i>string</i>   reference &lt;<i>statement-name</i>&gt;   syslog &lt;<i>syslog-tag</i>&gt;   tip cli <i>number</i>   topic &lt;<i>word</i>&gt; )&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. <b>apropos</b> option added in Junos OS Release 8.0.
<b>Description</b>	Display help about available operational commands, configuration statements, or general information about getting help. Entering the <b>help</b> command without an option provides introductory information about how to use the <b>help</b> and <b>?</b> commands.
<b>Options</b>	<p><b>apropos <i>string</i></b>—(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><b>reference &lt;<i>statement-name</i>&gt;</b>—(Optional) Display summary information for a configuration statement. This information is based on summary descriptions that appear in the Junos feature guides.</p> <p><b>syslog &lt;<i>syslog-tag</i>&gt;</b>—(Optional) Display information about system log messages.</p> <p><b>tip cli <i>number</i></b>—(Optional) Display a tip about using the CLI. Specify the number of the tip you want to view.</p> <p><b>topic &lt;<i>word</i>&gt;</b>—(Optional) Display usage guidelines for a topic or configuration statement. This information is based on subjects that appear in the Junos feature guides.</p>
<b>Required Privilege Level</b>	None
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Getting Online Help from the Junos OS Command-Line Interface on page 325</a></li> </ul>

## | (pipe)

<b>Syntax</b>	(compare   count   display (changed   commit-scripts   detail   display set   inheritance   omit   xml)   except <i>pattern</i>   find <i>pattern</i>   hold   last <i>lines</i>   match <i>pattern</i>   no-more   request message (all   <i>account@terminal</i> ) resolve <full-names>   save <i>filename</i>   trim <i>columns</i> )
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. display commit-scripts option added in Junos OS Release 7.4.
<b>Description</b>	Filter the output of an operational mode or a configuration mode command.
<b>Options</b>	<p><b>compare (filename   rollback <i>n</i> )</b>—(Configuration mode only, and only with the <b>show</b> command) Compare configuration changes with another configuration file.</p> <p><b>count</b>—Display the number of lines in the output.</p> <p><b>display</b>—Display additional information about the configuration contents.</p> <ul style="list-style-type: none"> <li><b>changed</b>—Tag changes with <b>junos:changed attribute</b> (XML only).</li> <li><b>commit-scripts</b>—(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>Configuration and Operations Automation Guide</i>.</li> <li><b>detail</b>—(Configuration mode only) Display configuration data detail.</li> <li><b>inheritance &lt;brief   default   no-comments   groups   terse&gt;</b>—(Configuration mode only) Display inherited configuration data and source group.</li> <li><b>omit</b>—(Configuration mode only) Display configuration statements omitted by the <b>apply-flags omit</b> configuration statement.</li> <li><b>set</b>—Display the configuration as a series of configuration mode commands required to re-create the configuration.</li> <li><b>xml</b>—(Operational mode only) Display the command output as Junos XML protocol (Extensible Markup Language [XML]) tags.</li> </ul> <p><b>except <i>pattern</i></b>—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.</p> <p><b>find <i>pattern</i></b>—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 (" ").</p> <p><b>last <i>lines</i></b>—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</p>

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 442](#).

**hold**—Hold text without exiting the **--More--** prompt.

**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**—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.

**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 426](#).

**trim *columns***—Trim specified number of columns from the start line.

**Required Privilege Level**

view

**Related Documentation**

- [Displaying the Current Junos OS Configuration on page 363](#).
- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 437](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 438](#)
- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 439](#)

## 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 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 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 [CLI Explorer](#).

**Additional Information** Most `request` commands are described in [CLI Explorer](#).

**Required Privilege Level** maintenance

**Related Documentation** • [Overview of Junos OS CLI Operational Mode Commands on page 413](#)

## restart

### List of Syntax [Syntax on page 552](#)

[Syntax \(ACX Series Routers\) on page 552](#)

[Syntax \(EX Series Switches\) on page 552](#)

[Syntax \(Routing Matrix\) on page 553](#)

[Syntax \(TX Matrix Routers\) on page 553](#)

[Syntax \(TX Matrix Plus Routers\) on page 553](#)

[Syntax \(MX Series Routers\) on page 553](#)

[Syntax \(QFX Series\) on page 554](#)

### 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 | 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 <logical-system logical-system-name> | sampling
 | sbc-configuration-process | sdk-service | service-deployment | services | services pgcp
 gateway gateway-name | 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 | mobile-ip |
 mountd-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 | mountd-service | multicast-snooping | pgm |
```

redundancy-interface-process | remote-operations | routing | secure-neighbor-discovery  
| service-deployment | sflow-service | snmp | vrrp | web-management>

**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>  
<all-chassis | all-lcc | lcc *number* | scc>  
<gracefully | immediately | soft>

**Syntax (TX Matrix Plus 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>  
<all-chassis | all-lcc | all-sfc | lcc *number* | sfc *number*>  
<gracefully | immediately | soft>

**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 | mobile-ip | mounstd-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 *logical-system-name*> |  
sampling | sbc-configuration-process | sdk-service | service-deployment | services | services  
pgcp gateway *gateway-name* | 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 | 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 | *logical-system-name*> | routing |  
 sampling | secure-neighbor-discovery | service-deployment | snmp | usb-control |  
 web-management>  
 <gracefully | immediately | soft>

**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 12.2 for ACX Series routers.  
 Options added:

- **dynamic-flow-capture** in Junos OS Release 7.4.
- **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) (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) (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 T1600 router that is connected to the TX Matrix Plus router. Replace **number** with a value from 0 through 3.

**license-service**—(EX Series switches) (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.

**mountd-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**—(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.

**vrp**—(EX Series switches and MX Series routers) (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) (Optional)  
Restart the Web management process.

**Required Privilege Level**    reset

**Related Documentation**    • [Overview of Junos OS CLI Operational Mode Commands on page 413](#)

**List of Sample Output**    [restart interfaces on page 561](#)

**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

---

<b>Syntax</b>	<code>set &lt;statement-path&gt; identifier</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Create a statement hierarchy and set identifier values. This is similar to <b>edit</b> except that your current level in the hierarchy does not change.
<b>Options</b>	<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>
<b>Required Privilege Level</b>	configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">edit on page 494</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>



---

## show

---

<b>Syntax</b>	<code>show &lt;statement-path&gt; &lt;identifier&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display the current configuration.
<b>Options</b>	<p><code>none</code>—Display the entire configuration at the current hierarchy level.</p> <p><i>identifier</i>—(Optional) Display the configuration for the specified identifier.</p> <p><i>statement-path</i>—(Optional) Display the configuration for the specified statement hierarchy path.</p>
<b>Required Privilege Level</b>	<code>configure</code> —To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show   display inheritance on page 567</a></li><li>• <a href="#">show   display omit on page 568</a></li><li>• <a href="#">show   display set on page 569</a></li><li>• <a href="#">show   display set relative on page 570</a></li><li>• <a href="#">show groups junos-defaults on page 571</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 363</a></li></ul>

## show configuration

---

<b>Syntax</b>	<code>show configuration</code> <code>&lt;statement-path&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display the configuration that currently is running on the router or switch, which is the last committed configuration.
<b>Options</b>	<p><b>none</b>—Display the entire configuration.</p> <p><b>statement-path</b>—(Optional) Display one of the following hierarchies in a configuration. (Each <b>statement-path</b> 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"><li>• <b>access</b>—Network access configuration.</li><li>• <b>access-profile</b>—Access profile configuration.</li><li>• <b>accounting-options</b>—Accounting data configuration.</li><li>• <b>applications</b>—Applications defined by protocol characteristics.</li><li>• <b>apply-groups</b>—Groups from which configuration data is inherited.</li><li>• <b>chassis</b>—Chassis configuration.</li><li>• <b>chassis network-services</b>—Current running mode.</li><li>• <b>class-of-service</b>—Class-of-service configuration.</li><li>• <b>diameter</b>—Diameter base protocol layer configuration.</li><li>• <b>ethernet-switching-options</b>—(EX Series switch only) Ethernet switching configuration.</li><li>• <b>event-options</b>—Event processing configuration.</li><li>• <b>firewall</b>—Firewall configuration.</li><li>• <b>forwarding-options</b>—Options that control packet sampling.</li><li>• <b>groups</b>—Configuration groups.</li><li>• <b>interfaces</b>—Interface configuration.</li><li>• <b>jsrc</b>—JSRC partition configuration.</li><li>• <b>jsrc-partition</b>—JSRC partition configuration.</li><li>• <b>logical-systems</b>—Logical system configuration.</li><li>• <b>poe</b>—(EX Series switch only) Power over Ethernet configuration.</li><li>• <b>policy-options</b>—Routing policy option configuration.</li><li>• <b>protocols</b>—Routing protocol configuration.</li></ul>

- **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 363](#)
- [Overview of Junos OS CLI Operational Mode Commands on page 413](#)

**List of Sample Output** [show configuration on page 565](#)  
[show configuration policy-options on page 566](#)

**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 alant version "8.2IO [builder]";
last changed: 2006-10-31 14:05:53 PST
system {
 host-name exhost;
 domain-name example.net;
 backup-router 192.1.1.254;
 time-zone America/Los_Angeles;
 default-address-selection;
 name-server {
 192.154.169.254;
 192.154.169.249;
```

```
 192.154.169.176;
 }
 services {
 telnet;
 }
 tacplus-server {
 1.2.3.4 {
 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 481](#)

## 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 563](#)

## show | display set

---

<b>Syntax</b>	show   display set
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Display the configuration as a series of configuration mode commands required to re-create the configuration from the top level of the hierarchy as <b>set</b> 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>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show on page 563</a></li><li>• <a href="#">Displaying set Commands from the Junos OS Configuration on page 367</a></li></ul>

## show | display set relative

---

**Syntax**    show | display set relative

**Release Information**    Command introduced before Junos OS Release 7.4.

**Description**    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
```

**Required Privilege Level**    view

**Related Documentation**    • [Displaying set Commands from the Junos OS Configuration on page 367](#)



---

## 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 481](#)

## show system commit

<b>Syntax</b>	show system commit
<b>Release Information</b>	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.
<b>Description</b>	Display the system commit history and any pending commit operation.
<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>• <i>clear system commit</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system commit on page 573</a> <a href="#">show system commit (At a Particular Time) on page 573</a> <a href="#">show system commit (At the Next Reboot) on page 573</a> <a href="#">show system commit (Rollback Pending) on page 573</a> <a href="#">show system commit (QFX Series) on page 573</a>
<b>Output Fields</b>	Table 53 on page 572 describes the output fields for the <b>show system commit</b> command. Output fields are listed in the approximate order in which they appear.

Table 53: show system commit Output Fields

Field Name	Field Description
<b>Commit history</b>	Displays the last 50 commit operations listed, most recent to first. The identifier <b>rescue</b> designates a configuration created for recovery using the <b>request system configuration rescue save</b> command.
<b>Timestamp</b>	Date and time of the commit operation.
<b>Username</b>	User who executed the commit operation.
<b>Commit method</b>	Method used to execute the commit operation: <ul style="list-style-type: none"> <li>• <b>cli</b>—CLI interactive user performed the commit operation.</li> <li>• <b>Junos XML protocol</b>—Junos XML protocol client performed the commit operation.</li> <li>• <b>synchronize</b>—The <b>commit synchronize</b> command was performed on the other Routing Engine.</li> <li>• <b>snmp</b>—An SNMP <b>set</b> request caused the commit operation.</li> <li>• <b>button</b>—A button on the router or switch was pressed to commit a rescue configuration for recovery.</li> <li>• <b>autoinstall</b>—A configuration obtained through autoinstallation was committed.</li> <li>• <b>other</b>—When there is no login name associated with the session, the values for user and client default to root and other. For example, during a reboot after package installation, mgd commits the configuration as a system commit, and there is no login associated with the commit.</li> </ul>

## Sample Output

### show system commit

```
user@host> show system commit
0 2003-07-28 19:14:04 PDT by root via other
1 2003-07-25 22:01:36 PDT by user via cli
2 2003-07-25 22:01:32 PDT by user via cli
3 2003-07-25 21:30:13 PDT by root via button
4 2003-07-25 13:46:48 PDT by user via cli
5 2003-07-25 05:33:21 PDT by root via autoinstall
...
rescue 2002-05-10 15:32:03 PDT by root via other
```

### show system commit (At a Particular Time)

```
user@host> show system commit
commit requested by root via cli at Tue May 7 15:59:00 2002
```

### show system commit (At the Next Reboot)

```
user@host> show system commit
commit requested by root via cli at reboot
```

### show system commit (Rollback Pending)

```
user@host> show system commit
0 2005-01-05 15:00:37 PST by root via cli commit confirmed, rollback in 3mins
```

### show system commit (QFX Series)

```
user@switch> show system commit
0 2011-11-25 19:17:49 PST by root via cli
```



## PART 4

# J-Web User Guide

- [Overview on page 577](#)
- [Configuring a Device Using J-Web on page 603](#)
- [Administering a Device Using J-Web on page 619](#)
- [Troubleshooting on page 651](#)



## CHAPTER 23

# Overview

- [Introduction to J-Web on page 577](#)
- [Understanding the J-Web User Interface on page 578](#)
- [Understanding Configuration Tools in J-Web on page 591](#)

## Introduction to J-Web

---

- [J-Web Overview on page 577](#)

### J-Web Overview

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the Juniper device 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 Juniper device, 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**—View the current configurations at a glance, configure the Juniper device, and manage configuration files. The J-Web interface provides the following different configuration methods:
  - Configure the Juniper device 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 Juniper device control traffic.

- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the Juniper devices.
- 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.

## Understanding the J-Web User Interface

---

- [Understanding the User Interfaces on page 578](#)
- [Starting the J-Web User Interface on page 581](#)
- [Understanding the J-Web Interface Layout on page 583](#)
- [J-Web Commit Options Guidelines on page 584](#)
- [Getting Help in the J-Web User Interface on page 585](#)
- [Establishing J-Web Sessions on page 586](#)
- [J-Web Layout on page 587](#)
- [Top Pane Elements on page 587](#)
- [Main Pane Elements on page 588](#)
- [Side Pane Elements on page 589](#)
- [Navigating the J-Web Interface on page 589](#)
- [Navigating the J-Web Configuration Editor on page 590](#)
- [Getting J-Web Help on page 590](#)

## Understanding the User Interfaces

You can use two user interfaces to configure, monitor, manage, and troubleshoot your device—the J-Web user interface and the command-line interface (CLI) for Junos OS.



**NOTE:** Other user interfaces facilitate the configuration of one or, in some cases, many devices on the network through a common API. Among the supported interfaces are the Junos Scope and Session and Resource Control (SRC) applications.

You can operate the device either in secure or router context. With the J-Web user interface and the CLI, you configure the routing protocols that run on the device and the device security features, including stateful firewall policies, Network Address Translation (NAT) attack prevention screens, Application Layer Gateways (ALGs), and IPsec VPNs. You also set the properties of its network interfaces. After activating a software configuration, you can use either user interface to monitor the system and the protocol traffic passing through the device, manage operations, and diagnose protocol and network connectivity problems.



This section contains the following topics:

- [J-Web User Interface on page 579](#)
- [CLI on page 580](#)

### J-Web User Interface

---

The J-Web user interface allows you to monitor, configure, troubleshoot, and manage your device 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 device, so you can fully configure it without using the CLI editor.

You can perform the following tasks with the J-Web user interface:

- **Dashboard (SRX Series devices only)**—Views high-level details of Chassis View, system identification, resource utilization, security resources, system alarms, file usage, login sessions, chassis status, threats activity, and storage usage.
- **Configuring**—View the current configurations at a glance, configure the device, and manage configuration files. The J-Web user interface provides the following configuration methods:
  - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
  - Edit the configuration in a text file.
  - Upload a configuration file.
  - Use wizards to configure basic setup, firewall, VPN, and NAT settings on all SRX Series devices.

The J-Web user interface also allows you to manage configuration history and set a rescue configuration.

- **Monitoring**—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- **Managing**—Manage log, temporary, and core (crash) files and schedule reboots on your devices. You can also manage software packages and licenses, and copy a snapshot of the system software to a backup device.
- **Diagnosing**—Diagnose routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze control traffic on the devices.
- **Configuring and monitoring events**—Filter and view system log messages that record events occurring on the device. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.
- **Configuring and monitoring alarms**—Monitor and diagnose the device by monitoring active alarms that alert you to the conditions on a network interface. You can also set the conditions that trigger alarms on an interface.

[Table 37 on page 302](#) shows the maximum number of concurrent J-Web sessions on SRX Series devices.

**Table 54: Concurrent J-Web Sessions on SRX Series Devices**

Device Type	Maximum Number of Users
SRX100	3
SRX110	3
SRX210	3
SRX220	5
SRX240	5
SRX550	5
SRX650	5
SRX1400	1024
SRX3400	1024
SRX3600	1024
SRX5400	1024
SRX5600	1024
SRX5800	1024

## CLI

The CLI is a straightforward command-line interface in which you type commands on a line and press Enter to execute them. The CLI provides command Help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the device, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the device. This topic refers to configuration mode as the *CLI configuration editor*.

[Table 38 on page 303](#) shows the maximum number of concurrent CLI sessions on SRX Series devices.

Table 55: Concurrent CLI Sessions on SRX Series Devices

Device Type	Maximum Number of Users
SRX100	6
SRX110	6
SRX210	4
SRX220	9
SRX240	6
SRX550	11
SRX650	11
SRX1400	250
SRX3400	250
SRX3600	250
SRX5400	250
SRX5600	250
SRX5800	250

- Related Documentation**
- [Starting the J-Web User Interface on page 581](#)
  - [Understanding the J-Web Interface Layout on page 583](#)
  - [Getting Help in the J-Web User Interface on page 585](#)
  - *CLI User Guide*

## 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.

[Table 56 on page 582](#) shows the maximum number of concurrent J-Web sessions on SRX Series devices.

**Table 56: Concurrent Web Sessions on SRX Series Devices**

Device Type	Maximum Number of Users
SRX100	3
SRX110	3
SRX210	3
SRX220	5
SRX240	5
SRX550	5
SRX650	5
SRX1400	1024
SRX3400	1024
SRX3600	1024
SRX5400	1024
SRX5600	1024
SRX5800	1024

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.

#### Related Documentation

- [Understanding the User Interfaces on page 301](#)
- [Understanding the J-Web Interface Layout on page 583](#)
- [J-Web Commit Options Guidelines on page 584](#)
- [Getting Help in the J-Web User Interface on page 585](#)
- [Establishing J-Web Sessions on page 586](#)

## Understanding the J-Web Interface Layout

The top pane of the J-Web user interface comprises the following elements:

- *hostname—model*—The hostname and model of the device are displayed in the upper-left corner.
- Logged in as: *username*—The username you used to log in to the device is displayed in the upper-left corner.
- Chassis—The chassis view of the device.
- Commit Options—A set of global options that allow you to commit multiple changes at the same time.
  - Commit—Commits the candidate configuration of the current user session, along with changes from other user sessions.
  - Compare—Displays the XML log of pending uncommitted configurations on the device.
  - Discard—Discards the candidate configuration of the current user session, along with changes from other user sessions.
  - Preference—Indicates your choice of committing all global configurations together or committing each configuration change immediately. The two behavior modes to which you can set your commit options are:
    - Validate and commit configuration changes—Sets the system to force an immediate commit on every screen after every configuration change.
    - Validate configuration changes—Loads all the configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode.
- Help—Links to information on Help and the J-Web user interface.
  - Help Contents—Displays context-sensitive Help topics.

- **About**—Displays information about the J-Web user interface, such as the version number.
- **Logout**—The Logout link, which ends your current login session and returns you to the login page, is available in the upper-right corner.
- **Taskbar**—A menu of J-Web tasks is displayed as tabs across the top of the J-Web user interface. Select a tab to access a task.
  - **Dashboard**—Displays current activity on the system.
  - **Configure**—Configures the device and views configuration history.
  - **Monitor**—Displays information about configuration and hardware on the device.
  - **Maintain**—Manages files and licenses, upgrades software, and reboots the device.
  - **Troubleshoot**—Troubleshoots network connectivity problems.

The main pane of the J-Web user interface includes the following elements to help you configure the device:

- **Red asterisk (\*)**—Appears next to all required fields.
- **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.

The left pane of the J-Web user interface displays subtasks related to the selected task in the J-Web taskbar.

#### Related Documentation

- [Understanding the User Interfaces on page 301](#)
- [Starting the J-Web User Interface on page 581](#)
- [J-Web Commit Options Guidelines on page 584](#)
- [Getting Help in the J-Web User Interface on page 585](#)
- [Establishing J-Web Sessions on page 586](#)

## 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.

#### Related Documentation

- [Understanding the User Interfaces on page 301](#)
- [Starting the J-Web User Interface on page 581](#)
- [Understanding the J-Web Interface Layout on page 583](#)
- [Getting Help in the J-Web User Interface on page 585](#)
- [Establishing J-Web Sessions on page 586](#)

## 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. You can navigate Help pages using hypertext links connecting related topics, or click the following options (if available) at the top and bottom of each page.
  - **Prev**—Access the previous page.
  - **Next**—Access the next page.
  - **Report an Error**—Access a form for providing feedback.
- **Wizard Help** (SRX100, SRX210, SRX220, SRX240, 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.

**Related Documentation**

- [Understanding the User Interfaces on page 301](#)
- [Starting the J-Web User Interface on page 581](#)
- [Understanding the J-Web Interface Layout on page 583](#)
- [J-Web Commit Options Guidelines on page 584](#)
- [Establishing J-Web Sessions on page 586](#)

## 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.

**Related Documentation**

- [Understanding the User Interfaces on page 301](#)
- [Starting the J-Web User Interface on page 581](#)
- [Understanding the J-Web Interface Layout on page 583](#)
- [J-Web Commit Options Guidelines on page 584](#)



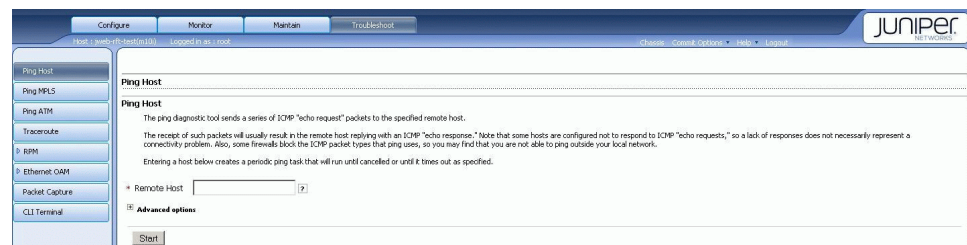
- [Getting Help in the J-Web User Interface on page 585](#)

## J-Web Layout

Each page of the J-Web interface is divided into the following panes, as shown in [Figure 24 on page 587](#).

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, troubleshoot, and manage the Juniper 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.

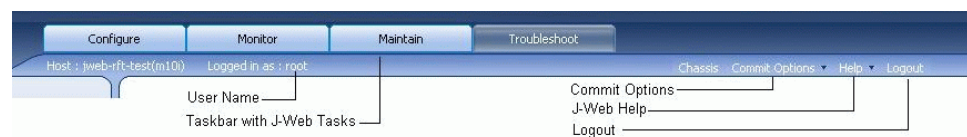
Figure 24: J-Web Layout



## Top Pane Elements

The top pane comprises the elements shown in [Figure 25 on page 587](#).

Figure 25: Top Pane Elements



- *hostname – model*—Hostname and model of the Juniper device.
- Logged in as: *username*—Username you used to log in to the Juniper 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 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 Juniper device by using Configuration pages or the configuration editor, and view configuration history.
  - **Monitor**—View information about configuration and hardware on the Juniper device.
  - **Maintain**—Manage files and licenses, upgrade software, and reboot the Juniper device.
  - **Troubleshoot**—Troubleshoot network connectivity problems.

## Main Pane Elements

The main pane comprises the elements shown in [Figure 26 on page 588](#).

**Figure 26: Main Pane Elements**

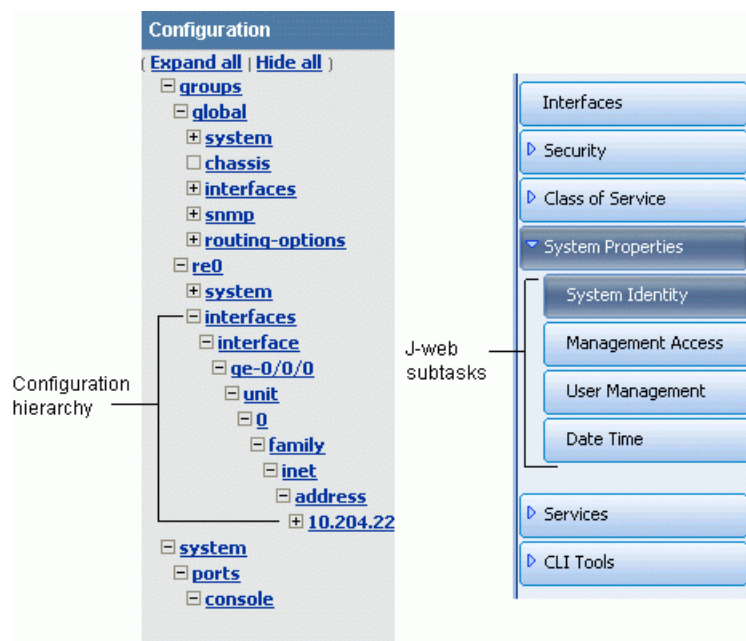
- Help (?) icon—Displays useful information when you move the cursor over the question mark. This help displays field-specific information, such as the definition, format, and valid range of the field.
- Red asterisk (\*)—Indicates a required field.
- Icon Legend— For the Edit Configuration subtask (J-Web configuration editor) only, explains icons that appear in the user interface to provide information about configuration statements:

- C—Comment. Move your cursor over the icon to view a comment about the configuration statement.
- I—Inactive. The configuration statement does not affect the Juniper device.
- M—Modified. The configuration statement is added or modified.
- \*—Mandatory. The configuration statement must have a value.

## Side Pane Elements

The side pane comprises the elements shown in [Figure 27 on page 589](#).

**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 Juniper 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.

## Navigating the J-Web Interface

The layout of the panes allows you to quickly navigate through the interface. You navigate the J-Web interface, move forward and backward, scroll pages, and expand and collapse elements as you do in a typical Web browser interface.

From the taskbar, select the J-Web task that you want to perform. Selecting the task displays related subtasks in the side pane. When you select a subtask, related fields are displayed in the main pane. By default, the system selects the first subtask and displays its related fields in the main pane. The side pane and taskbar are available from all pages, allowing you to skip from one task or subtask to the other from any page in the interface.

You can easily navigate to most subtasks by selecting them from the side pane. On pages where you are required to take an action, buttons and links allow you to move to the next or previous page as you perform certain actions. For more information, see [“Navigating the J-Web Configuration Editor” on page 590](#).

## Navigating the J-Web Configuration Editor

When you select **Configure>CLI Tools>Point and Click CLI** (J-Web configuration editor), the side pane displays the top level of the configured hierarchy committed on the Juniper device. The main pane displays the configuration hierarchy options.

You can click a statement or identifier displayed in the main pane, or in the hierarchy in the left pane, to display the corresponding configuration options in the main pane. For more information, see [“Point and Click CLI \(J-Web Configuration Editor\)” on page 593](#).

After typing or selecting your configuration edits, click a button in the main pane (described in [Table 57 on page 590](#)) to move to the previous page after applying or committing the configuration. An updated configuration does not take effect until you commit it.

**Table 57: Key J-Web Edit Configuration Buttons**

Function	Button
Apply edits to the candidate configuration, and return one level up (previous page) in the configuration hierarchy.	<b>OK</b>
Clear the entries you have not yet applied to the candidate configuration, and return one level up (previous page) in the configuration hierarchy.	<b>Cancel</b>
Verify edits and apply them to the current configuration file running on the Juniper device. For more details, see <a href="#">“Committing a Configuration” on page 615</a> .	<b>Commit</b>
Discard changes or delete configuration.	<b>Discard</b>

## Getting J-Web Help

The J-Web interface provides two ways to display Help for the Monitor, Configure, Troubleshoot, and Maintain tasks.

To get Help in the J-Web interface:

- **Field-sensitive Help**—Move the cursor over the question mark (?) next to the field for which you want more information. The system displays useful information about the field. 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 field 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. You can navigate Help pages using hypertext links connecting related topics, or click the following options (if available) at the top and bottom of each page. [Figure 28 on page 591](#) shows Help for the CoS Configuration page.
- **Prev**—Access the previous page.
- **Next**—Access the next page.
- **Report an Error**—Access a form for providing feedback.

**Figure 28: CoS Help Page**



## Understanding Configuration Tools in J-Web

- [Configuration Task Overview on page 591](#)
- [Point and Click CLI \(J-Web Configuration Editor\) on page 593](#)
- [CLI Viewer \(View Configuration Text\) on page 595](#)
- [CLI Editor \(Edit Configuration Text\) on page 597](#)
- [CLI Terminal Requirements on page 598](#)
- [Starting the CLI Terminal on page 598](#)
- [Using the CLI Terminal on page 599](#)

### Configuration Task Overview

The J-Web user interface provides different methods for configuring your Juniper device with the Junos OS. Choose a configuration method appropriate to your needs and familiarity with the interface.

Use the J-Web user interface to configure the services supported on a Juniper device, including system settings, routing protocols, interfaces, network management, and user access.

Alternatively, you can configure the Juniper device services with the Junos OS command-line interface (CLI) from a console connection to the Juniper device or a remote

network connection. You can also access the CLI from the J-Web interface. For more information, see [“Using the CLI Terminal” on page 599](#). For complete information about using the CLI, see the *CLI User Guide*.

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 through the user interface immediately, but do not take effect on the Juniper device until you *commit* the changes.

You can set your preference by selecting **Commit** or **Commit Check**. This preference is applicable across sessions and users. **Commit Check** only validates the configuration and reports errors. **Commit** validates and commits the configuration specified on every J-Web page.

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, all changes made by all the users take effect. If you are editing the configuration with the CLI, you can edit an *exclusive* or *private* candidate configuration. For more information, see the *CLI User Guide*.

When you commit a configuration, the Juniper device saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49. You can roll back the configuration to any saved version.



**NOTE:** You must assign a root password before committing a configuration and can do so on the J-Web Set Up page.

To better understand the Junos OS configuration process, become familiar with the terms defined in [Table 58 on page 592](#).

**Table 58: Junos OS Configuration Terms**

Term	Definition
<b>candidate configuration</b>	A working copy of the configuration that can be edited without affecting the Juniper device until it is committed.
<b>configuration group</b>	Group of configuration statements that can be inherited by the rest of the configuration.
<b>commit a configuration</b>	Have the candidate configuration checked for proper syntax, activated, and marked as the current configuration file running on the Juniper device.
<b>configuration hierarchy</b>	Set of hierarchically organized configuration statements that make up the Junos OS configuration on a Juniper device. There are two types of statements: <i>container statements</i> , which contain other statements, and <i>leaf statements</i> , which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.
<b>roll back a configuration</b>	Return to a previously committed configuration.

## Point and Click CLI (J-Web Configuration Editor)

Using Point and Click CLI, you can configure all properties of the Junos OS, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

The configuration is stored as a hierarchy of statements. You create the specific hierarchy of configuration statements that you want to use. After you finish entering the configuration statements, you commit them to activate the configuration on the Juniper device.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the Juniper device and then committed. Edit Configuration (J-Web configuration editor) allows you to create the hierarchy interactively, and Edit Configuration Text allows you to create and commit statements as an ASCII text file.

To access Edit Configuration, also called the J-Web configuration editor, select **Configure>CLI Tools>Point and Click**. 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](#)

The Edit Configuration page allows you to configure all Juniper device services that you can configure from the Junos OS CLI. Each field in the J-Web configuration editor has the same name as the corresponding configuration statement at the same hierarchy level in the CLI. For example, the Policy Options field corresponds to the **policy-options** statement in the CLI. As a result, you can easily switch from one interface to the other or follow a CLI configuration example using the J-Web configuration editor.

[Table 59 on page 593](#) lists key J-Web configuration editor tasks and their functions.

**Table 59: J-Web Configuration Editor Tasks Summary**

J-Web Configuration Editor Task	Function
<b>Access</b>	Configure network access. For example, you can configure the Point-to-Point Protocol (PPP), the tracing access processes, the Layer 2 Tunneling Protocol (L2TP), RADIUS authentication for L2TP, and Internet Key Exchange (IKE) access profiles.
<b>Accounting options</b>	Configure accounting profiles. An accounting profile represents common characteristics of collected accounting data, including collection interval, accounting data files, and counter names on which to collect statistics. On the Accounting options pages, you can configure multiple accounting profiles, such as the interface, filter, MIB, routing engine, and class usage profiles.
<b>Applications</b>	Define applications by protocol characteristics and group the applications you have defined into a set. On the Applications pages, you can configure application properties, such as Internet Control Message Protocol (ICMP) code and type. You can also specify application protocols—also known as application-level gateways (ALGs)—to be included in an application set for service processing, or specify network protocols to match in an application definition.

Table 59: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
<b>Chassis</b>	Configure Juniper device chassis properties. On the Chassis pages, you can configure different properties of the Juniper device chassis, including conditions that activate the red and yellow alarm LEDs on the Juniper devices and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs).
<b>Class of service</b>	Define class-of-service (CoS) components, such as CoS value aliases, classifiers, forwarding classes, rewrite rules, schedulers, and virtual channel groups. The Class of service pages also allow you to assign CoS components to interfaces. For more information, see the <i>Class of Service Feature Guide for Security Devices</i> .
<b>Diameter</b>	Configure Diameter base protocol. For example, you can specify the remote peers, the endpoint origin attributes, and network elements that associate routes with peers. .
<b>Event options</b>	Configure event policies. An event policy is an if-then-else construct that defines actions to be executed by the software on receipt of a system log message. For each policy, you can configure multiple actions, as follows—ignore the event, upload a file to a specified destination, execute Junos OS operational mode commands, or execute Junos OS event scripts (op scripts). For more information, see the <i>Configuration and Operations Automation Guide</i> .
<b>Firewall</b>	Configure stateless firewall filters. With stateless firewall filters—also known as ACLs—you can control packets transiting the Juniper device to a network destination and packets destined for and sent by the Juniper device. On the Firewall pages, you can create filters and add terms to them. For each term, you can set the match conditions and associate actions to be performed on packets matching these conditions.
<b>Forwarding options</b>	<p>Configure traffic forwarding and traffic sampling options. You can sample IP traffic based on particular input interfaces and various fields in the packet header. You can also use traffic sampling to monitor any combination of specific logical interfaces, specific protocols on one or more interfaces, a range of addresses on a logical interface, or individual IP addresses.</p> <p>Traffic forwarding policies allow you to control the per-flow load balancing, port mirroring, and Domain Name System (DNS) or Trivial File Transfer Protocol (TFTP) forwarding.</p>
<b>Interfaces</b>	Configure physical and logical interface properties. For the physical interface on the Juniper device, you can modify default values for general interface properties, such as the interface's maximum transmission unit (MTU) size, link operational mode, and clock source. For each logical interface, you can specify the protocol family and other logical interface properties. For more information, see the <i>Interfaces Feature Guide for Security Devices</i> .
<b>Jsrc</b>	Configure Jsrc. For example, you can configure the JSRC partition, associate a Diameter instance, SAE hostname, and the SAE realm with the partition.
<b>Policy options</b>	Configure policies by specifying match conditions and associating actions with the conditions. On the Policy options page, you can create a named community and define autonomous system (AS) paths, damping parameters, and routing policies. You can also create a named prefix list and include it in a routing policy.
<b>Protocols</b>	Configure routing protocols such as Border Gateway Protocol (BGP), Distance Vector Multicast Routing Protocol (DVMRP), Intermediate System-to-Intermediate System (IS-IS), Multiprotocol Label Switching (MPLS), Open Shortest Path First (OSPF), Resource Reservation Protocol (RSVP) and Routing Information Protocol (RIP). For more information, see the <i>Junos OS Routing Protocols Library for Security Devices</i> and the <i>MPLS Feature Guide for Security Devices</i> .



Table 59: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
<b>Routing instances</b>	<p>Configure routing instances. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. On the Routing instances pages, you can configure the following types of routing instances: forwarding, Layer 2 virtual private network (VPN), nonforwarding, VPN routing and forwarding (VRF), virtual router, and virtual private LAN service (VPLS). For more information, see the <i>Junos OS Routing Protocols Library for Security Devices</i>.</p>
<b>Routing options</b>	<p>Configure protocol-independent routing options that affect systemwide routing operations. On the Routing options pages, you can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Add routing table entries, including static routes, aggregated (coalesced) routes, generated routes (routes of last resort), and martian routes (routes to ignore).</li> <li>• Create additional routing tables and routing table groups.</li> <li>• Set the AS number of the Juniper device for use by BGP.</li> <li>• Set the router ID, which is used by BGP and OSPF to identify the Juniper device from which a packet originated.</li> <li>• Define BGP confederation members for use by BGP.</li> <li>• Configure how much system logging information to log for the routing protocol process.</li> <li>• Configure systemwide tracing (debugging) to track standard and unusual routing operations and record this information in a log file.</li> </ul> <p>For more information, see the <i>Junos OS Routing Protocols Library for Security Devices</i>.</p>
<b>Security</b>	<p>Configure Internet Protocol Security (IPsec) for authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, you can configure the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). You can also configure the SSH known host list, and the trace options for IPsec key management. For more information, see the <i>VPN Feature Guide for Security Devices</i>.</p>
<b>Services</b>	<p>Configure application settings for services interfaces, such as dynamic flow capture parameters, the intrusion detection service (IDS), IPsec VPN service, RPM, stateful firewalls, and Network Address Translation (NAT).</p>
<b>Snmp</b>	<p>Configure SNMP to monitor network devices from a central location. You can specify an administrative contact and location and add a description for each system being managed by SNMP. You can also configure SNMP community strings, trap options, and interfaces on which SNMP requests can be accepted. For more information, see the <i>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices</i>.</p>
<b>System</b>	<p>Configure system management functions, including the router's hostname, address, and domain name; the addresses of Domain Name System (DNS) servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; and properties of the router's auxiliary and console ports.</p>

## CLI Viewer (View Configuration Text)

To view the entire configuration in text format, select **Configure>CLI Tools>CLI Viewer**. The main pane displays the configuration in text format (see [Figure 29 on page 596](#)). The displayed configuration is the same as the configuration displayed when you enter the Junos OS CLI command **show configuration**.

**Figure 29: View Configuration Text Page****CLI Viewer**

The CLI Viewer page shows the current configuration running on the device.

The current configuration running on the device is

```
Last commit: 2010-01-11 03:52:56 PST by user.
version 10.1B3.4;
groups {
 re0 {
 system {
 host-name tp5;
 backup-router 192.168.71.254 destination 0.0.0.0/0;
 }
 interfaces {
 fxp0 {
 unit 0 {
 family inet {
 address 192.168.70.147/21;
 }
 }
 }
 }
 }
 re1 {
 system {
 backup-router 192.168.71.254 destination 0.0.0.0/0;
 }
 }
 global {
 system {
 domain-name device12.example.com;
 }
 }
}
```

The configuration statements appear in a fixed order, irrespective of the order in which you configured the Juniper device. The top of the configuration displays a timestamp indicating when the configuration was last changed and the current version.

[Figure 29 on page 596](#) shows that user **regress** committed the last configuration on 11 January 2010, and the software version running on the Juniper device is Junos OS Release 10.1.

Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off 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 displayed. Each leaf statement ends with a semicolon (**;**), as does the last statement in the hierarchy.

This indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indentation and use of new lines are not required in ASCII configuration files.

## CLI Editor (Edit Configuration Text)

Using View and Edit, you can configure all properties of the Junos OS, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

The configuration is stored as a hierarchy of statements. You create the specific hierarchy of configuration statements that you want to use. After you finish entering the configuration statements, you commit them to activate the configuration on the Juniper device.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the Juniper device and then committed. Edit Configuration (J-Web configuration editor) allows you to create the hierarchy interactively, and Edit Configuration Text allows you to create and commit statements as an ASCII text file.

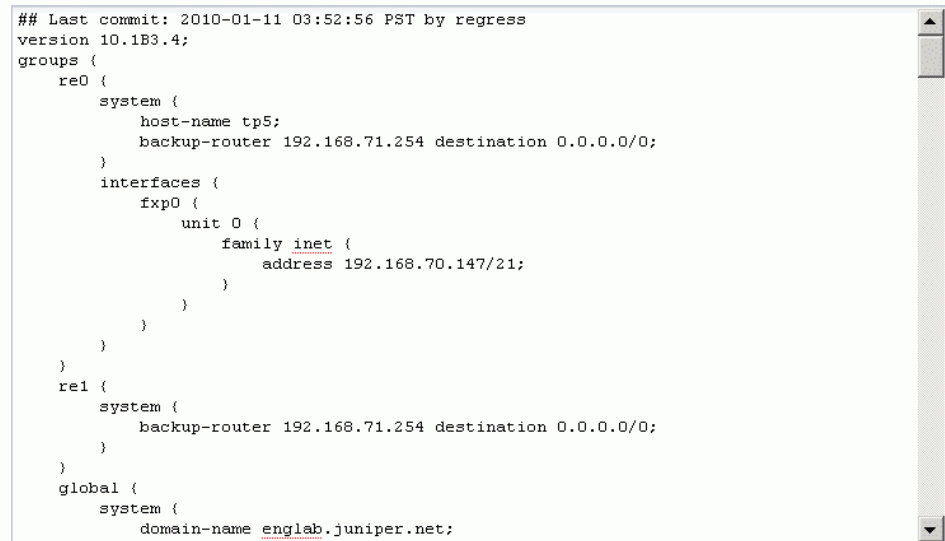
To edit the entire configuration in text format, select **Configure>CLI Tools>CLI Editor**. The main pane displays the configuration in a text editor (see [Figure 30 on page 597](#)).

**Figure 30: Edit Configuration Text Page**

### CLIEditor

Edit the configuration. When you click "Commit", the edited configuration replaces the existing configuration and takes effect. If any errors occur when the configuration is loading or committed, they are displayed and the previous configuration is restored.

### Configuration:



```
Last commit: 2010-01-11 03:52:56 PST by regress
version 10.1B3.4;
groups {
 re0 {
 system {
 host-name tp5;
 backup-router 192.168.71.254 destination 0.0.0.0/0;
 }
 interfaces {
 fxp0 {
 unit 0 {
 family inet {
 address 192.168.70.147/21;
 }
 }
 }
 }
 }
 re1 {
 system {
 backup-router 192.168.71.254 destination 0.0.0.0/0;
 }
 }
 global {
 system {
 domain-name englab.juniper.net;
 }
 }
}
```

For more information about the format of an ASCII configuration file, see [“CLI Viewer \(View Configuration Text\)” on page 595](#).



**CAUTION:** We recommend that you use this method to edit and commit the configuration only if you have experience editing configurations through the CLI.

To edit the entire configuration in text format:

1. Navigate to the hierarchy level you want to edit.
2. Edit the candidate configuration using standard text editor operations—insert lines (with the Enter key), delete lines, and modify, copy, and paste text.
3. Click **Commit** to load and commit the configuration.

The Juniper device checks the configuration for the correct syntax before committing it.

When you edit the ASCII configuration file, you can add comments of one or more lines. Comments 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 after a statement or on a separate line following a statement, they are removed when you click Commit. Comments must begin and end with special characters. For more information, see the *CLI User Guide*.

## CLI Terminal Requirements

To access the CLI through the J-Web interface, your management device requires the following features:

- SSH access—Enable SSH on your system. SSH provides a secured method of logging in to the Juniper device, to encrypt traffic so that it is not intercepted. If SSH is not enabled on the system, the CLI terminal page displays an error and provides a link to the Set Up Quick Configuration page that allows you to enable SSH. For more information, see “[Configuring Basic Settings](#)” on page 609.
- Java applet support—Make sure that your Web browser supports Java applets.
- JRE installed on the client—Install Java Runtime Environment (JRE) version 1.4 or later on your system. JRE is a software package that must be installed on a system to run Java applications. Download the latest JRE version from the Java Software website <http://www.java.com/>. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.



**NOTE:** The CLI terminal is supported on JRE version 1.4 and later only.

---

## Starting the CLI Terminal

To get started on the CLI terminal:

1. Make sure that your system meets the requirements mentioned in “[CLI Terminal Requirements](#)” on page 598.
2. In the J-Web interface, select **Troubleshoot > CLI Terminal**. A Java applet is downloaded into the J-Web interface allowing SSH access to the Juniper device.
3. Log in to the CLI by typing your Junos OS password. This is the same password that you use to log in to the J-Web interface.

After you log in, a percentage sign (%) prompt appears to indicate that you are in the UNIX shell (see [Figure 31 on page 599](#)).

4. To start the CLI, type **cli**.

The presence of the angle bracket (>) prompt indicates that the CLI has started. By default, the prompt is preceded by a string that contains your username and the hostname of the Juniper device. The angle bracket also indicates that you are in operational mode.

5. To enter configuration mode, type **configure**. The **[edit]** prompt indicates the current configuration mode.
6. Type **exit** or **quit** to return to the previous level of the configuration—for example, to return to operational mode from configuration mode.

For security purposes, each time you log out of the Juniper device or leave the CLI terminal page, the CLI terminal session ends and you are required to reenter your password. When you select **Troubleshoot>CLI Terminal** again, retype your Junos OS password to access the CLI.

**Figure 31: Starting the CLI Terminal**

#### CLI Terminal

A Java applet will be loaded below that will provide an SSH connection between your browser and '10.209.8.129'. You will be asked to enter your password again as a security measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

```
root@betsy% cli
root@betsy> configure
Entering configuration mode

[edit]
root@betsy# exit
Exiting configuration mode

root@betsy> quit
root@betsy% █
```

## Using the CLI Terminal

The Junos OS CLI uses industry-standard tools and utilities to provide a set of commands for monitoring and configuring a Juniper device. You type commands on a line and press Enter to execute them. The CLI provides command help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The J-Web CLI terminal provides access to the Junos OS CLI through the J-Web interface. The functionality and behavior of the CLI available through the CLI terminal page is the same as the Junos OS CLI available through the Juniper device console. The CLI terminal supports all CLI commands and other features such as CLI help and autocompletion. Using the CLI terminal page, you can fully configure, monitor, and manage your Juniper device.

The commands in the CLI are organized hierarchically, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the Juniper device system and system software are grouped under the **show** command, and all commands that display information about the routing table are grouped under the **show route** command. The hierarchical organization results in commands that have a regular syntax and provides the following features that 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 they are operating on. 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.
- Command completion—Command completion for command names (keywords) and command options is also available at each level of the hierarchy. In the CLI terminal, you can do one of the following for command completions:
  - Type a partial command name followed immediately by a question mark (with no intervening space) to see a list of commands that match the partial name you typed.
  - Press the Spacebar to complete a command or option that you have partially typed. 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.

The Tab key option is currently not available on the CLI terminal.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the Juniper device, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the Juniper device.

For more information about the Junos OS CLI, see the *CLI User Guide*. For information about configuring and monitoring Junos OS features with the CLI, see <http://www.juniper.net/books>.

Figure 32 on page 601 shows the CLI terminal displaying all the options that you can configure in CLI configuration mode.

Figure 32: J-Web CLI Terminal

**CLI Terminal**

A Java applet will be loaded below that will provide an SSH connection between your browser and '10.209.8.129'. You will be asked to enter your password again as a security measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

```
root@betsy# set ?
Possible completions:
> access Network access configuration
> access-profile Access profile for this instance
> accounting-options Accounting data configuration
> applications Define applications by protocol characteristics
+ apply-groups Groups from which to inherit configuration data
> chassis Chassis configuration
> class-of-service Class-of-service configuration
> event-options Event processing configuration
> firewall Define a firewall configuration
> forwarding-options Configure options to control packet forwarding
> 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
> security Security configuration
> services
> snmp Simple Network Management Protocol configuration
> system System parameters
[edit]
root@betsy#
```





## CHAPTER 24

# Configuring a Device Using J-Web

- [Installing and Starting J-Web on page 603](#)
- [Configuring Secure Web Access to a Device on page 605](#)
- [Configuring a Device Using J-Web on page 608](#)

### Installing and Starting J-Web

---

- [J-Web Software Requirements on page 603](#)
- [Installing the J-Web Software on page 603](#)
- [Starting the J-Web Interface on page 604](#)

### 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 device comes with the Junos OS installed on it. When you power on the Juniper device, all software starts automatically. On M Series and T Series routers, you need to install the J-Web software because it is not shipped on the Juniper device.

If your Juniper 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 Juniper device. After the installation, you must enable Web management of the Juniper device with the CLI.



**NOTE:** M Series or T Series routers must be running Junos OS version 7.3 or later to support the J-Web interface.

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 Juniper device.
4. Copy the software package to the Juniper device. We recommend that you copy it to the `/var/tmp` directory.
5. If you have previously installed the J-Web software on the Juniper 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 Juniper 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 Juniper device. From configuration mode in the CLI, enter the following command:

```
user@host# system services web-management http
```

## Starting the J-Web Interface

Before you start the user interface, you must perform the initial Juniper device configuration described in the Juniper device hardware guide. After the initial configuration, you use your username and password and the hostname or IP address of the router to start the user interface.

To start the J-Web interface:

1. Launch a Web browser that has Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

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 a certificate on the Juniper device and enabled HTTPS.



**NOTE:** If the Juniper 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 Juniper device.

2. After **http://** or **https://** in your Web browser, type the hostname or IP address of the Juniper device, and press Enter.

The J-Web login page appears.

3. On the login page, 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.

The J-Web **Initial Configuration Set Up** page appears.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

## Configuring Secure Web Access to a Device

- [Secure Web Access Overview on page 605](#)
- [Generating SSL Certificates on page 605](#)
- [Configuring Secure Web Access on page 606](#)

### Secure Web Access Overview

A Juniper device uses the Secure Sockets Layer (SSL) protocol to provide secure management of Juniper 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 Juniper 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 Juniper 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 Juniper device through HTTPS.

Without SSL encryption, communication between your Juniper 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 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 606 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.

Figure 33 on page 606 shows the Edit Management Access page.

**Figure 33: Edit Management Access Page**

The figure displays two panels of the 'Edit Management Access' configuration interface. The left panel is the 'Services' tab, showing checkboxes for 'Enable telnet', 'Enable SSH', 'Enable HTTP', and 'Enable HTTPS'. It also includes a 'JUNOScript' section with options to 'Enable JUNOScript over clear text' and 'Enable JUNOScript over SSL', and a dropdown for 'JUNOScript certificate'. The 'Enable HTTP' section has a 'Selected interfaces' list and an 'Available interfaces' list (ge-0/0/0.0, lo0.0). The 'Enable HTTPS' section has a 'HTTPS certificate' dropdown, an 'Enable on all interfaces' checkbox, and another 'Selected interfaces' list. The right panel is the 'Certificates' tab, featuring a 'Certificate names' list with 'Add...', 'Edit...', and 'Delete' buttons. Below is an 'Add certificate' section with fields for 'Certificate name:' and 'Certificate content:', and a 'Save' button. Both panels have 'OK' and 'Cancel' buttons at the bottom.

To configure Web access settings in the J-Web interface:

1. Enter information into the Edit Management Access page, as described in [Table 60 on page 607](#).
2. Click **OK** to apply the configuration.
3. To verify that Web access is enabled correctly, connect to the router 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 JUNOScript access—A JUNOScript client such as Junos Scope is required. For information about how to log in to Junos Scope, see the *Junos Scope Software User Guide*.

Table 60: Secure Access Configuration Summary

Field	Function	Your Action
<b>Adding Certificates</b>		
Certificate names	<p>Displays digital certificates required for SSL access to the Juniper device.</p> <p>Allows you to add and delete SSL certificates.</p> <p>For information about how to generate an SSL certificate, see <a href="#">“Generating SSL Certificates” on page 605</a>.</p>	<p>To add a certificate:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b> on the Certificates tab to display the Add certificate box.</li> <li>2. Type a name in the Certificate name box—for example, <b>new</b>.</li> <li>3. Paste the generated certificate and RSA private key in the Certificate content box.</li> </ol> <p>To delete a certificate, select it from the list and click <b>Delete</b>.</p>
<b>Enabling HTTP Web Access</b>		
Enable HTTP	Enables HTTP access on interfaces.	To enable HTTP access, select the <b>Enable HTTP access</b> check box on the Services tab.
Enable HTTP on all interfaces	Enables HTTP access on all interfaces at one time.	To enable HTTP access on all interfaces, select the <b>Enable on all interfaces</b> check box on the Services tab.
Selected interfaces	Lists the interfaces for which you want to enable HTTP access.	<p>Clear the <b>Enable on all interfaces</b> check box on the Services tab, select the interface, and move it to the appropriate list by clicking the direction arrows:</p> <ul style="list-style-type: none"> <li>• To enable HTTP access on an interface, move the interface to the <b>Selected interfaces</b> list.</li> <li>• To disable HTTP access on an interface, move the interface to the <b>Available interfaces</b> list.</li> </ul>
<b>Enabling HTTPS Web Access</b>		
Enable HTTPS	Enables HTTPS access on interfaces.	To enable HTTPS access, select the <b>Enable HTTPS access</b> check box on the Services tab.

Table 60: Secure Access Configuration Summary (*continued*)

Field	Function	Your Action
HTTPS certificate	Specifies SSL certificates to be used for encryption.  This field is available only after you have created an SSL certificate.	To specify the HTTPS certificate, select a certificate from the HTTPS certificate list on the Services tab—for example, <b>new</b> .
Enable on all interfaces	Enables HTTPS on all interfaces at one time.	To enable HTTPS on all interfaces, select the <b>Enable HTTPS on all interfaces</b> check box on the Services tab.
Selected interfaces	Lists interfaces for which you want to enable HTTPS access.	Clear the <b>Enable on all interfaces</b> check box on the Services tab, select the interface, and move it to the appropriate list by clicking the direction arrows: <ul style="list-style-type: none"> <li>To enable HTTPS access on an interface, move the interface to the <b>Selected interfaces</b> list.</li> <li>To disable HTTPS access on an interface, move the interface to the <b>Available interfaces</b> list.</li> </ul>
<b>Enabling JUNOScript over SSL</b>		
Enable JUNOScript over SSL	Enables secured SSL access to the JUNOScript XML scripting API.	To enable SSL access, select the <b>Enable JUNOScript over SSL</b> check box on the Services tab.
JUNOScript certificate	Specifies SSL certificates to be used for encryption.  This field is available only after you create at least one SSL certificate.	To enable an SSL certificate, select a certificate from the JUNOScript certificate list on the Services tab—for example, <b>new</b> .

## Configuring a Device Using J-Web

- [Configuring Basic Settings on page 609](#)
- [Editing and Committing a Junos OS Configuration on page 612](#)
- [J-Web Configuration Tasks on page 612](#)
- [Editing a Configuration on page 613](#)
- [Committing a Configuration on page 615](#)
- [Discarding Parts of a Candidate Configuration on page 616](#)
- [Accounting Options on page 616](#)

## Configuring Basic Settings

Before you begin initial configuration, complete the following tasks:

- Install the Juniper device in its permanent location, as described in the hardware installation guide or the Getting Started Guide for your Juniper 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 34 on page 610](#)), as described in [Table 61 on page 610](#).
2. Click **Apply** to apply the configuration.

Figure 34: 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 61: Initial Configuration Set Up Summary

Field	Function	Your Action
<b>Identification</b>		
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.  <b>NOTE:</b> 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.
<b>Time</b>		
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 <b>Add</b> .  To delete an IP address, click it in the box above the Add button, then click <b>Delete</b> .



Table 61: 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"> <li>To immediately set the time using the NTP server, click <b>Set Time via NTP</b>. The router sends a request to the NTP server and synchronizes the system time.</li> <li><b>NOTE:</b> If you are configuring other settings on this page, the router also synchronizes the system time using the NTP server when you click <b>Apply</b>.</li> <li>To set the time manually, click <b>Set Time Manually</b>. A pop-up window allows you to select the current date and time from lists.</li> </ul>
<b>Network</b>		
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 <b>Add</b>.</p> <p>To delete an IP address, click it in the box above the Add button, then click <b>Delete</b>.</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 <b>Add</b>.</p> <p>To delete a domain name, click it in the box above the Add button, then click <b>Delete</b>.</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 <b>127.0.0.1/32</b> .	Type a 32-bit IP address and prefix length, in dotted decimal notation.
<b>fe-0/0/0</b> Address (on J2300, J4300, and J6300 routers) <b>ge-0/0/0</b> Address (on J4350 and J6350 routers) <b>fxp0</b> Address (on M Series routers)	Defines the IP address and prefix length of the management interface. The management interface is used for accessing the router. The DHCP client sets this address to <b>192.168.1.1/24</b> if no DHCP server is found.	<p>Type a 32-bit IP address and prefix length, in dotted decimal notation.</p> <p><b>NOTE:</b> You must enter the address for the management interface on the Quick Configuration Set Up page before you click <b>Apply</b>. If you do not manually configure this address, you will lose your connection to the J-Web interface when you click <b>Apply</b>.</p>
<b>Management Access</b>		
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.

Table 61: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
Allow SSH Access	Allows remote access to the router by using SSH.	To enable SSH access, select the check box.

## Editing and Committing a Junos OS Configuration

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 through the user interface immediately, but do not take effect on the Juniper device until you *commit* the changes.

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, all changes made by all the users take effect. If you are editing the configuration with the CLI, you can edit an *exclusive* or *private* candidate configuration. For more information, see the *CLI User Guide*.

When you commit a configuration, the Juniper device saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49. You can roll back the configuration to any saved version.



**NOTE:** You must assign a root password before committing a configuration and can do so on the J-Web Set Up page.

## J-Web Configuration Tasks

J-Web configuration pages offer you several different ways to configure your Juniper device. Configuration pages provide access to all the configuration statements supported by the Juniper 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 62 on page 612 provides a summary of the J-Web configuration tasks.

Table 62: J-Web Configuration Tasks 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.	"Point and Click CLI (J-Web Configuration Editor)" on page 593
Edit the configuration in text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	"CLI Editor (Edit Configuration Text)" on page 597

Table 62: J-Web Configuration Tasks Summary (*continued*)

J-Web Configuration Task	Description	More Information
Upload a configuration file	Upload a complete configuration.	"Upload Configuration File" on page 624
View the configuration in text format	View the entire configuration on the Juniper device in text format.	"CLI Viewer (View Configuration Text)" on page 595

## 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 35 on page 613](#)).

Figure 35: Edit Configuration Page

**Configuration**  
Expand all | Hide all |  
groups  
system

**Configuration**  
Refresh Commit... Discard...

Access [Configure](#)  
Accounting options [Configure](#)  
Applications [Configure](#)  
Chassis [Configure](#)  
Class of service [Configure](#)  
Diameter [Configure](#)  
Event options [Configure](#)  
Firewall [Configure](#)  
Forwarding options [Configure](#)  
Interfaces [Configure](#)  
Jsrc [Configure](#)  
Policy options [Configure](#)  
Protocols [Configure](#)  
Routing instances [Configure](#)  
Routing options [Configure](#)  
Security [Configure](#)  
Services [Configure](#)  
Snmp [Configure](#)  
System [Edit](#) [Delete](#)

**Access profile**  
Access profile name  ?

**Jsrc partition**  
Jsrc partition name  ?

**Advanced**  
Apply groups [Add new entry](#)

Value	Actions
global	<a href="#">Edit</a> <a href="#">Delete</a>
re0	<a href="#">Edit</a> <a href="#">Delete</a>

Refresh Commit... Discard...

**Icon Legend**

- C Comment**  
The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
- I Inactive**  
The configuration statement is not active and does not affect the device.
- M Modified**  
The configuration statement has been changed or added.
- Mandatory**  
The configuration statement must have a value.

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 63 on page 614](#) 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 63: J-Web Edit Configuration Links**

Link	Function
<b>Add new entry</b>	Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.
<b>Configure</b>	Displays information for a configuration option that has not been configured, allowing you to include a statement.
<b>Delete</b>	Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.
<b>Edit</b>	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 64 on page 614](#) describes the meaning of these icons.

**Table 64: J-Web Edit Configuration Icons**

Icon	Meaning
<b>C</b>	Displays a comment about a statement.
<b>I</b>	Indicates that a statement is inactive.

Table 64: J-Web Edit Configuration Icons (*continued*)

Icon	Meaning
<b>M</b>	Indicates that a statement has been added or modified, but has not been committed.
<b>*</b>	Indicates that the statement or identifier is required in the configuration.
<b>?</b>	Provides help information.



**NOTE:** You can annotate statements with comments or make them inactive only through the CLI. For more information, see the *CLI User Guide*.

After typing or selecting your configuration edits, click a button in the main pane (described in [Table 65 on page 615](#)) to apply your changes or refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

Table 65: J-Web Edit Configuration Buttons

Button	Function
<b>OK</b>	Applies edits to the candidate configuration, and returns you to the previous level in the configuration hierarchy.
<b>Cancel</b>	Clears the entries you have not yet applied to the candidate configuration, and returns you to the previous level in the configuration hierarchy.
<b>Refresh</b>	Updates the display with any changes to the configuration made by other users. .
<b>Commit</b>	Verifies edits and applies them to the current configuration file running on the Juniper device. For details, see <a href="#">“Committing a Configuration” on page 615</a> .
<b>Discard</b>	Removes edits applied to, or deletes existing statements or identifiers from, the candidate configuration. For details, see <a href="#">“Discarding Parts of a Candidate Configuration” on page 616</a> .

## 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 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. To display a list of users, see [“Displaying Users Editing the Configuration” on page 621](#). For more information about editing an exclusive candidate configuration, see the *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**.

## Discarding Parts of a Candidate Configuration

Before committing a candidate configuration, you can discard changes you applied or delete existing statements or identifiers.

To discard parts of a candidate configuration:

1. Navigate to the level of the hierarchy you want to edit, and click **Discard**.

The main pane displays a list of target statements based on the hierarchy level and the changes you have made.

2. Select an option button to specify the appropriate discard operation or deletion. (Not all buttons appear in all situations.)

- **Discard Changes Below This Point**—Discards changes made to the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a discarded statement are also discarded.
- **Discard All Changes**—Discards all changes made to the candidate configuration.
- **Delete Configuration Below This Point**—Deletes all changes and statements in the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a deleted statement are also deleted.

3. To confirm the discard operation or deletion, click **Discard**.

The updated candidate configuration does not take effect on the Juniper device until you commit it.

## Accounting Options

[Figure 36 on page 617](#) shows the Accounting options configuration page. This page displays the different settings that you can configure at the accounting options hierarchy level.

On the Accounting options page, click any option to view and configure related options.

Figure 36: Accounting Options Configuration Editor Page

**Configuration**

**Accounting options**

OK Cancel Refresh Commit... Discard...

**Class usage profile** (None configured) [Add new entry](#)

**File** (None configured) [Add new entry](#)

**Filter profile** (None configured) [Add new entry](#)

**Interface profile** (None configured) [Add new entry](#)

**Mib profile** (None configured) [Add new entry](#)

**Policy decision statistics profile** (None configured) [Add new entry](#)

**Routing engine profile** (None configured) [Add new entry](#)

**Advanced**

OK Cancel Refresh Commit... Discard...

**Icon Legend**

- C Comment**  
The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
- I Inactive**  
The configuration statement is not active and does not affect the device.
- M Modified**  
The configuration statement has been changed or added.
- \* Mandatory**  
The configuration statement must have a value.

Each field in the J-Web configuration editor has the same name as the corresponding configuration statement at the same hierarchy level in the CLI. The options on this page match the options displayed when you enter **edit accounting options** in the CLI:

```
user@router# edit accounting-options ?
Possible completions:
 <[Enter]> Execute this command
 > class-usage-profile Class usage profile for accounting data
 > file Accounting data file configuration
 > filter-profile Filter profile for accounting data
 > interface-profile Interface profile for accounting data
 > mib-profile MIB profile for accounting data
 > policy-decision-statistics-profile
 Profile for policy decision bulkstats
 > routing-engine-profile Routing Engine profile for accounting data
 | Pipe through a command

[edit]
```





## CHAPTER 25

# Administering a Device Using J-Web

- [Managing Configurations and Files on a Device on page 619](#)
- [Managing Software on a Device on page 626](#)
- [Configuring and Viewing Alarms on a Device on page 627](#)
- [Viewing and Filtering System Log Events on a Device on page 630](#)
- [Monitoring a Device on page 636](#)
- [Managing J-Web Sessions and Users on page 649](#)

### Managing Configurations and Files on a Device

---

- [Displaying Configuration History on page 619](#)
- [Displaying Users Editing the Configuration on page 621](#)
- [Loading a Previous Configuration File on page 622](#)
- [Downloading a Configuration File on page 623](#)
- [Comparing Configuration Files on page 623](#)
- [Upload Configuration File on page 624](#)
- [Using Files on page 625](#)

### Displaying Configuration History

When you commit a configuration, the Juniper device saves the current operational version and the previous 49 versions of committed configurations. To manage these configuration files with the J-Web interface, select **Maintain>Config Management>History**. The main pane displays Database Information and Configuration History (see [Figure 37 on page 620](#)).

[Table 66 on page 620](#) summarizes the contents of the display.

The configuration history display allows you to perform the following operations:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the Juniper device.

Figure 37: Configuration Database and History Page

**History**

---

**Database Information**

No users are editing the configuration database.

---

**Configuration History**

The following table shows the device's commit history.

To view a configuration, click the revision number.

To compare configurations, select two and click "Compare".

	Number	Date/Time	User	Client	Comment	Log Message	Action
<input type="checkbox"/>	<a href="#">Current</a>	2008-12-23 09:28:24 UTC	regress	cli			<a href="#">Download</a>
<input type="checkbox"/>	<a href="#">1</a>	2008-12-23 08:16:34 UTC	root	junoscript		Rolled back via Web Interface	<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">2</a>	2008-12-22 08:33:12 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">3</a>	2008-12-22 08:30:49 UTC	root	other			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">4</a>	2008-09-30 07:04:28 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">5</a>	2008-09-30 06:46:52 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">6</a>	2008-09-30 06:44:48 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">7</a>	2008-09-30 06:40:08 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>
<input type="checkbox"/>	<a href="#">8</a>	2008-03-19 19:31:53 UTC	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>

Table 66: J-Web Configuration History Summary

Field	Description
Number	Version of the configuration file.
Date/Time	Date and time the configuration was committed.
User	Name of the user who committed the configuration.

Table 66: J-Web Configuration History Summary (*continued*)

Field	Description
Client	<p>Method by which the configuration was committed:</p> <ul style="list-style-type: none"> <li>• <b>cli</b>—A user entered a Junos OS CLI command.</li> <li>• <b>junoscript</b>—A JUNOScript client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way.</li> <li>• <b>snmp</b>—An SNMP <b>set</b> request started the operation.</li> <li>• <b>button</b>—The CONFIG button on the router was pressed to commit the rescue configuration (if set) or to clear all configurations except the factory configuration.</li> <li>• <b>autoinstall</b>—Autoinstallation was performed.</li> <li>• <b>other</b>—Another method was used to commit the configuration.</li> </ul>
Comment	Comment.
Log Message	<p>Method used to edit the configuration:</p> <ul style="list-style-type: none"> <li>• <b>Imported via paste</b>—Configuration was edited and loaded with the <b>Configuration&gt;View and Edit&gt;Edit Configuration Text</b> option. For more information, see <a href="#">“CLI Editor (Edit Configuration Text)” on page 597</a>.</li> <li>• <b>Imported upload [filename]</b>—Configuration was uploaded with the <b>Configuration&gt;View and Edit&gt;Upload Configuration File</b> option. For more information, see <a href="#">“Upload Configuration File” on page 624</a>.</li> <li>• <b>Modified via quick-configuration</b>—Configuration was modified with the J-Web Quick Configuration tool specified by <i>quick-configuration</i>.</li> <li>• <b>Rolled back via user-interface</b>—Configuration was rolled back to a previous version through the user interface specified by <i>user-interface</i>, which can be <b>Web Interface</b> or <b>CLI</b>. For more information, see <a href="#">“Loading a Previous Configuration File” on page 622</a>.</li> </ul>
Action	Action to perform with the configuration file. The action can be <b>Download</b> or <b>Rollback</b> . For more information, see <a href="#">“Downloading a Configuration File” on page 623</a> and <a href="#">“Loading a Previous Configuration File” on page 622</a> .

For more information about saved versions of configuration files, see [“Editing and Committing a Junos OS Configuration” on page 612](#).

## Displaying Users Editing the Configuration

To display a list of users editing the Juniper device configuration, select **Maintain>Config Management>History**. The list is displayed as Database Information in the main pane (see [Figure 38 on page 622](#)). [Table 67 on page 622](#) summarizes the Database Information display.

Figure 38: Database Information Page

<b>History</b>						
<b>Database Information</b>						
The following users are editing the configuration:						
User Name	Start Time	Idle Time	Terminal	PID	Edit Flags	Edit Path
rob	2007-01-31 19:18:37 PST	16:16:14	p1	3423	None	[edit]
joe	2007-02-22 02:58:45 PST	13:56:25	p0	2962	None	[edit]
<b>Configuration History</b>						
The following table shows the router's commit history.						
To view a configuration, click the revision number.						

Table 67: J-Web Configuration Database Information Summary

Field	Description
User Name	Name of user editing the configuration.
Start Time	Time of day the user logged in to the Juniper device.
Idle Time	Elapsed time since the user issued a configuration command from the CLI.
Terminal	Terminal on which the user is logged in.
PID	Process identifier assigned to the user by the Juniper device.
Edit Flags	Designates a private or exclusive edit.
Edit Path	Level of the configuration hierarchy that the user is editing.

### Loading a Previous Configuration File

To load (roll back) and commit a previous configuration file stored on the Juniper device:

1. In the Action column, click **Rollback** for the version of the configuration you want to load.

The main pane displays the results of the rollback operation.



**NOTE:** When you click **Rollback**, the Juniper device loads and commits the selected configuration. This behavior is different from entering the **rollback configuration mode** command from the CLI, where the configuration is loaded, but not committed.

## Downloading a Configuration File

To download a configuration file from the Juniper device to your local system:

1. In the Action column, click **Download** for the version of the configuration you want to download.
2. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

## Comparing Configuration Files

To compare any two of the past 50 committed configuration files:

1. Click two of the check boxes to the left of the configuration versions you want to compare.
2. Click **Compare**.

The main pane displays the differences between the two configuration files at each hierarchy level as follows (see [Figure 39 on page 624](#)):

- Lines that have changed are highlighted side by side in green.
- Lines that exist only in the more recent configuration file are displayed in red on the left.
- Lines that exist only in the least recent configuration file are displayed in blue on the right.

Figure 39: J-Web Configuration File Comparison Results

**History****Compare Rollback 5 Configuration to Rollback 2 Configuration**

Rollback 5 Configuration		Rollback 2 Configuration	
[edit]		[edit]	
version 9.1B2.8;		version "9.410 [builder]";	
		system {	
		domain-name englab.juniper.net;	
		domain-search [ englab.juniper.net juniper.net jnpr.net spglab.juniper.net ];	
		backup-router 10.209.63.254;	
		services {	
		rlogin;	
		rsh;	
		ssh;	
		telnet;	
		web-management {	
		http;	
		}	
		}	
		routing-options {	
		static {	
		route 0.0.0.0/0 next-hop 10.209.63.254;	
		}	
		}	

**Upload Configuration File**

To upload a configuration file from your local system:

1. Select **Maintain>Config Management>Upload**.

The main pane displays the File to Upload box (see [Figure 40 on page 625](#)).

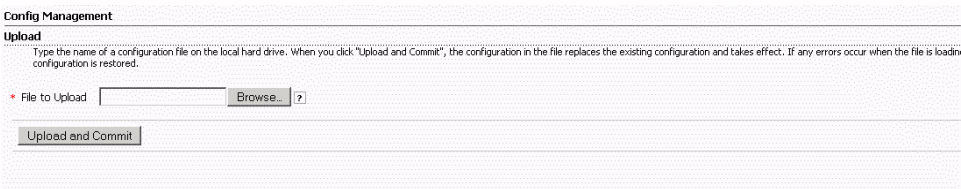
2. Specify the name of the file to upload using one of the following methods:

- Type the absolute path and filename in the File to Upload box.
- Click **Browse** to navigate to the file.

3. Click **Upload and Commit** to upload and commit the configuration.

The Juniper device checks the configuration for the correct syntax before committing it.

Figure 40: J-Web Upload Configuration File Page



Using Files

Select **Maintain>Files** in the J-Web interface to manage log, temporary, and core files on the Juniper device.

[Table 68 on page 625](#) lists the different tasks that you can perform from the **Maintain>Files** page.

Table 68: Manage Files Tasks Summary

Manage Files Task	Functions
Clean Up Files	<p>Rotate log files and delete unnecessary files on the Juniper device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.</p> <p>The file cleanup procedure performs the following tasks. Click <b>Clean Up Files</b> to begin.</p> <ul style="list-style-type: none"><li>• Rotates log files—All information in the current log files is archived, and fresh log files are created.</li><li>• Deletes log files in <b>/cf/var/log</b>—Any files that are not currently being written to are deleted.</li><li>• Deletes temporary files in <b>/cf/var/tmp</b>—Any files that have not been accessed within two days are deleted.</li><li>• Deletes all crash files in <b>/cf/var/crash</b>—Any core files that the router has written during an error are deleted.</li></ul> <p>Alternatively, you can rotate log files and display the files that you can delete by entering the <b>request system storage cleanup</b> command at the J-Web CLI terminal. For more information, see <a href="#">“Using the CLI Terminal” on page 599</a>. For more information about the <b>request system storage cleanup</b> command, see <a href="#">CLI Explorer</a>.</p>

Table 68: Manage Files Tasks Summary (*continued*)

Manage Files Task	Functions
<b>Download and Delete Files</b>	<p>Download a copy of an individual file or delete it from the Juniper device. When you download a file, it is not deleted from the file system. When you delete the file, it is permanently removed.</p> <p>Click one of the following file types, and then select whether to download or delete a file:</p> <ul style="list-style-type: none"> <li>• <b>Log Files</b>—Lists the log files located in the <code>/cf/var/log</code> directory on the router.</li> <li>• <b>Temporary Files</b>—Lists the temporary files located in the <code>/cf/var/tmp</code> directory on the router.</li> <li>• <b>Old Junos OS</b>—Lists the existing Junos OS packages in the <code>/cf/var/sw</code> directory on the router.</li> <li>• <b>Crash (Core) Files</b>—Lists the core files located in the <code>/cf/var/crash</code> directory on the router.</li> </ul> <p><b>CAUTION:</b> If you are unsure whether to delete a file from the router, we recommend using the <b>Clean Up Files</b> task, which determines the files that can be safely deleted from the file system.</p>
<b>Delete Backup Junos Package</b>	<p>Delete a backup copy of the previous software installation from the Juniper device. When you delete the file, it is permanently removed from the file system.</p> <p>Click <b>Delete backup Junos Package</b> to begin.</p>

## Managing Software on a Device

- [Sample Task—Manage Snapshots on page 626](#)
- [Using Reboot on page 627](#)

### Sample Task—Manage Snapshots

[Figure 41 on page 627](#) shows a **Maintain>Snapshot** page that allows you to back up the currently running and active file system on a standby storage device that is not running. In this example, you are taking the snapshot to replace the current primary boot device on the Juniper device.

To take the snapshot:

1. Select **Maintain>Snapshot** from the task bar.
2. Next to Advanced options, click the expand icon (see [Figure 41 on page 627](#)).
3. Select **compact-flash** from the Target Media list to specify the storage device to copy the snapshot to.
4. Next to As Primary Media, select the check box to create a storage medium to be used in the internal compact flash slot only.
5. Click **Snapshot**.



Figure 41: Manage Snapshots Page

Snapshot

System Snapshot

You can configure boot devices to replace the primary boot device or to act as a backup boot device. To do this, you create a snapshot of the running system software, saving the snapshot to an alternate media.

The snapshot process copies the current system software, along with the current and rescue configurations, to alternate media. Optionally, you can copy only the factory and rescue configurations.

Target Media: Snapshots the system software to specified media:

- compact-flash: Internal compact flash
- removable-compact-flash: External compact flash

Target Media  ?

Factory ☐ ?

Partition ☐ ?

**Advanced options**

As Primary Media ☒ ?

Data Size  ?

Swap Size  ?

Config Size  ?

Root Size  ?

## Using Reboot

The Maintain>Reboot page allows you to reboot the Juniper device at a specified time. Using the Maintain>Reboot page, you can perform the following tasks:

- Reboot the router immediately, after a specified number of minutes or at the absolute time that you specify, on the current day.
- Stop (halt) the router software immediately. After the router software has stopped, you can access the router through the console port only.
- Type a message to be displayed to any users on the router before the reboot occurs.

Click **Schedule** to begin.

If the reboot is scheduled to occur immediately, the router reboots. You cannot access the J-Web interface until the router 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.

Alternatively, you can reboot the Juniper device by running the **request system reboot** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 599](#). For more information about the **request system reboot** command, see [CLI Explorer](#).

## Configuring and Viewing Alarms on a Device

- [Using Alarms on page 628](#)
- [View Alarms on page 628](#)
- [Active Alarms Information on page 628](#)
- [Alarm Severity on page 629](#)

- [Displaying Alarm Descriptions on page 629](#)
- [Sample Task—Viewing and Filtering Alarms on page 629](#)

## Using Alarms

You can monitor active alarms on the J-Web interface. The View Alarms page alerts you about conditions that might prevent the Juniper device from operating normally. The page displays information about active alarms, the severity of the alarms, the time at which the alarm began, and a brief description for each active alarm. Alternatively, you can use the CLI to view alarms on all Juniper devices. An alarm indicates that you are running the Juniper device in a manner that is not recommended. When you see an alarm, you must check its cause and remedy it.

Alternatively, you can display alarm information by entering the following commands at the J-Web CLI terminal:

- **show chassis alarms**
- **show system alarms**

For more information, see [“Using the CLI Terminal” on page 599](#). For more information about the commands, see [CLI Explorer](#).

## View Alarms

To view the alarms page, click **Monitor > Events and Alarms > Alarms**. The View Alarms page alerts you about conditions that might prevent the Juniper device from operating normally. The page displays information about active alarms, the severity of the alarms, the time at which the alarm began and a brief description for each active alarm. Alternatively, you can use the CLI to view alarms on all routers. An alarm indicates that you are running the Juniper device in a manner that is not recommended. When you see an alarm, you must check its cause and remedy it.

Alternatively, you can display alarm information by entering the following commands at the J-Web CLI terminal:

- **show chassis alarms**
- **show system alarms**

The View Alarms page displays all the active alarms along with detailed descriptions. Each description provides more information about the probable cause or solution for the condition that caused the alarm (see [“Sample Task—Viewing and Filtering Alarms” on page 629](#)). The description also provides the date and time when the failure was detected.

## Active Alarms Information

The View Alarms page displays the following types of alarms. You can set the conditions that trigger alarms on an interface. Chassis and system alarm conditions are preset.

- **Interface alarms**—Indicate a problem in the state of the physical links on a fixed or installed Physical Interface Module (PIM), such as a link failure or a missing signal. To enable interface alarms, you must configure them.

- Chassis alarms—Indicate a failure on the Juniper device or one of its components, such as a power supply failure, excessive component temperature, or media failure. 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.

## Alarm Severity

Alarms displayed on the View Alarms page can have the following two severity levels:

- Major (red)—Indicates a critical situation on the Juniper 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 Juniper 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.

## Displaying Alarm Descriptions

All active alarms are displayed on the View Alarms page with detailed description of the alarm. This description provides more information about the probable cause or solution for the condition that caused the alarm (see [“Sample Task—Viewing and Filtering Alarms” on page 629](#)). The description also provides the date and time when the failure was detected. Note the date and time of an alarm so that you can correlate it with error messages on the View Events page or in the messages system log file.

## Sample Task—Viewing and Filtering Alarms

[Figure 42 on page 630](#) shows the View Alarms page displaying one system alarm that is currently active. The yellow color indicates that the alarm is noncritical. You can also see the time at which the system received the alarm. You can also filter alarms based on alarm type, severity, description, and date.

Figure 42: View Alarms Page

**View Alarms**

**Alarm filter**

Alarm type:  Severity:

Description:

Date From:  To:

**Alarm Details**

Type	Severity	Description	Time
System	Minor	Rescue configuration is not set	2008-12-22 08:31:01 UTC

## Viewing and Filtering System Log Events on a Device

- [Using View Events on page 630](#)
- [Viewing Events on page 631](#)
- [View Events on page 631](#)
- [Understanding Severity Levels on page 632](#)
- [Using Filters on page 632](#)
- [Using Regular Expressions on page 634](#)
- [Sample Task—Filtering and Viewing Events on page 635](#)

### Using View Events

The Events task on the J-Web interface enables you to filter and view system log messages that record events occurring on your Juniper device.

[Figure 43 on page 631](#) shows the View Events page. This page provides an easy method to view the events recorded in the system log (also known as system log messages). By default, the View Events page displays a summary of the most recent 25 events, with severity levels highlighted in different colors.

The events summary includes information about the time the event occurred, the name of the process that generated the message, the event ID, and a short description of the event. You can move the cursor over the question mark (?) next to an event ID to display a useful description of the event.

You can filter events by system log filename, event ID, text from the event description, name of the process that generated the event, or time period, to display only the events you want. You can also generate and save an HTML report of the system alarms.

Alternatively, enter the following command in the J-Web CLI terminal to display the list of messages and a brief description of each message. For more information about the CLI terminal, see [“Using the CLI Terminal” on page 599](#).

user@host> help syslog ?

Figure 43: View Events page

View Events

Events Filter

System Log File: messages

Process:

☐ Include archived files

Date From: 2009-07-17,03:42

To: 2009-07-17,04:42

Event ID:

Description:

Search

Reset

Events Detail

Generate Report

Process	Severity	Event ID	Event Description	Time
xrtpd			kernel time sync enabled 2001	2009-07-17 04:38:58 PDT
xrtpd			kernel time sync enabled 6001	2009-07-17 04:21:55 PDT
checklogin	notice	WEB_AUTH_SUCC	Authenticated http client (username root)	2009-07-17 04:09:54 PDT

Viewing Events

The View Events page displays system log messages that record events occurring on the Juniper device. Events recorded include those of the following types:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as Juniper device power-off due to excessive temperature

For more information about system log messages, see the [System Log Explorer](#).

View Events

To view system log messages that record events occurring on your Juniper device, click **Monitor>Events and Alarms>View Events**. The View Events page is displayed. This page provides an easy method to view the events recorded in the system log (also known as system log messages). By default, the View Events page displays a summary of the most recent 25 events, with severity levels highlighted in different colors.

The View Events page displays system log messages that record events occurring on the Juniper device. Events recorded include those of the following types:

- Routine operations, such as creation of an OSPF protocol adjacency or a user login into the configuration database

- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as Juniper device power-off due to excessive temperature

On the View Events page, you can also use filters to display relevant events. [Table 70 on page 633](#) lists the different filters, their functions, and the associated actions. You can apply any or a combination of the described filters to view the messages that you want to view. After specifying the filter or filters you want, click **Search** to display the filtered events.

## Understanding Severity Levels

On the View Events page, the severity level of a message is indicated by different colors. The severity level indicates how seriously the triggering event affects Juniper device functions.

[Table 69 on page 632](#) lists the system log severity levels, the corresponding colors, and a description of what the severity level indicates.

**Table 69: Severity Levels**

Color	Severity Level (from Highest to Lowest Severity)	Description
Red	<b>emergency</b>	System panic or other conditions that cause the Juniper device to stop functioning.
Orange	<b>alert</b>	Conditions that must be corrected immediately, such as a corrupted system database.
Pink	<b>critical</b>	Critical conditions, such as hard drive errors.
Blue	<b>error</b>	Standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
Yellow	<b>warning</b>	Conditions that warrant monitoring.
Green	<b>notice</b>	Conditions that are not error conditions but are of interest or might warrant special handling.
	<b>info</b>	Informational messages. This is the default.
	<b>debug</b>	Software debugging messages.
Gray	<b>unknown</b>	No severity level is specified.

## Using Filters

On the View Events page, you can use filters to display relevant events.

[Table 70 on page 633](#) lists the different filters, their functions, and the associated actions.

You can apply any or a combination of the described filters to view the messages that you want to view. After specifying the filter or filters you want, click **Search** to display the filtered events. Click **Reset** to clear the existing search criteria and enter new values.

**Table 70: Summary of Event Filters**

Event Filter	Function	Your Action
<b>System Log File</b>	<p>Specifies the name of a system log file for which you want to display the recorded events.</p> <p>The list includes the names of all the system log files that you configure.</p> <p>By default, a log file, <b>messages</b>, is included in the <b>/var/log/</b> directory.</p> <p>For information about how to configure system log files, see the <a href="#">System Log Explorer</a>.</p>	To specify events recorded in a particular file, select the system log filename from the list—for example, <b>messages</b> .
<b>Event ID</b>	<p>Specifies the event ID for which you want to display the messages.</p> <p>If you type part of the ID, the system completes the remaining ID automatically.</p> <p>An event ID, also known as a system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.</p>	To specify events with a specific ID, type its partial or complete ID—for example, <b>TFTPD_AF_ERR</b> .
<b>Description</b>	<p>Specifies text from the description of events that you want to display.</p> <p>You can use a regular expression to match text from the event description.</p> <p><b>NOTE:</b> The regular expression matching is case-sensitive.</p> <p>For more information about using regular expressions, see <a href="#">“Using Regular Expressions” on page 634</a>.</p>	<p>To specify events with a specific description, type a text string from the description. You can include a regular expression.</p> <p>For example, type <b>^Initial*</b> to display all messages with lines beginning with the term <i>Initial</i>.</p>
<b>Process</b>	<p>Specifies the name of the process generating the events you want to display.</p> <p>To view all the processes running on your system, enter the CLI command <b>show system processes</b> in the J-Web CLI terminal.</p> <p>For more information about processes, see the <i>Installation and Upgrade Guide for Security Devices</i>.</p>	<p>To specify events generated by a process, type the name of the process.</p> <p>For example, type <b>mgd</b> to list all messages generated by the management process.</p>
<b>Include archived files</b>	Includes the archived log files in the search. Files are archived when the active log file reaches its maximum size limit.	Select the check box to include archived files in the search.

Table 70: Summary of Event Filters (*continued*)

Event Filter	Function	Your Action
<b>Date From</b>	Specifies the time period in which the events you want displayed are generated.	To specify the time period:
<b>To</b>	<p>A calendar allows you to select the year, month, day, and time. It also allows you to select the local time.</p> <p>By default, the messages generated in the last one hour are displayed. <b>To</b> shows the current date and time, and <b>Date From</b> shows the time one hour before end time.</p>	<ul style="list-style-type: none"> <li>Click the button next to <b>Date From</b> and select the year, month, date, and time—for example, <b>02/10/2006 11:32</b>.</li> <li>Click the button next to <b>To</b> and select the year, month, date, and time—for example, <b>02/10/2006 3:32</b>.</li> </ul> <p>To select the current time as the start time, select <b>Local Time</b>.</p>

## Using Regular Expressions

On the View Events page, you can filter the events displayed by the text in the event description. In the **Description** box, you can use regular expressions to filter and display a set of messages for viewing. Junos OS supports POSIX Standard 1003.2 for extended (modern) UNIX regular expressions.

Table 71 on page 634 specifies some of the commonly used regular expression operators and the terms matched by them. A term can match either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.



**NOTE:** On the View Events page, the regular expression matching is case-sensitive.

Table 71: Common Regular Expression Operators and the Terms They Match

Regular Expression Operator	Matching Terms
. (period)	<p>One instance of any character except the space.</p> <p>For example, <code>.in</code> matches messages with <i>win</i> or <i>windows</i>.</p>
* (asterisk)	<p>Zero or more instances of the immediately preceding term.</p> <p>For example, <code>tre*</code> matches messages with <i>tree</i>, <i>tread</i>, or <i>trough</i>.</p>
+ (plus sign)	<p>One or more instances of the immediately preceding term.</p> <p>For example, <code>tre+</code> matches messages with <i>tree</i> or <i>tread</i> but not <i>trough</i>.</p>
? (question mark)	<p>Zero or one instance of the immediately preceding term.</p> <p>For example, <code>colou?r</code> matches messages with <i>or color</i> or <i>colour</i>.</p>
(pipe)	<p>One of the terms that appear on either side of the pipe operator.</p> <p>For example, <code>gre ay</code> matches messages with either <i>grey</i> or <i>gray</i>.</p>



Table 71: Common Regular Expression Operators and the Terms They Match (*continued*)

Regular Expression Operator	Matching Terms
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is specific to Junos OS.
^ (caret)	The start of a line, when the caret appears outside square brackets.  For example, <code>^T</code> matches messages with <i>This line</i> and not with <i>On this line</i> .
\$ (dollar sign)	Strings at the end of a line.  For example, <code>:\$</code> matches messages with <i>the following:</i> and not with <i>2:00</i> .
[] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range.  For example, <code>[0-9]</code> matches messages with any number.
() (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.  For example, <code>dev(/ ice)</code> matches messages with <i>dev/</i> or <i>device</i> .

### Sample Task—Filtering and Viewing Events

Figure 44 on page 636 shows the View Events page displaying filtered events. In this example, you are typing **UI\_CHILD\_EXITED** in the Event ID box and clicking **Search**. The Event Summary displays messages with the **UI\_CHILD\_EXITED** event ID only. You can view the following information about the events:

- Messages displayed are green. The green color and context-sensitive help indicate that the message severity level is **notice** and the event type is **error**. This information means that the condition causing the message is an error or failure and might require corrective action.
- The events were generated by the management process (mgd).
- The Event Description column displays a brief description of the event, and the help description provides information about the cause of the event.

Figure 44: J-Web View Events Page

**View Events**

**Events Filter**

System Log File:  Process:

☐ Include archived files

Date From:  To:

Event ID:  Description:

**Events Detail**

Process	Severity	Event ID	Event Description	Time
checklogin	notice	WEB_AUTH_SUC	Authenticated httpd client (username root)	2009-07-17 04:09:54 PDT

## Monitoring a Device

- [Monitor Task Overview on page 636](#)
- [Class of Service on page 637](#)
- [Interfaces on page 637](#)
- [MPLS on page 638](#)
- [RPM on page 639](#)
- [Routing on page 640](#)
- [Security on page 641](#)
- [Service Sets on page 643](#)
- [Services on page 643](#)
- [System View on page 644](#)
- [Sample Task—Monitoring Interfaces on page 645](#)
- [Sample Task—Monitoring Route Information on page 647](#)

## Monitor Task Overview

Use the J-Web Monitor tasks to monitor your Juniper device. The J-Web interface displays diagnostic information about the Juniper device in the browser.

You can also monitor the Juniper device with command-line interface (CLI) operational mode commands that you type into a CLI emulator in the J-Web interface. The monitoring pages display the same information displayed in the output of **show** commands entered in the CLI terminal. For more information about the J-Web CLI terminal, see [“Using the CLI Terminal” on page 599](#). For more information about the **show** commands, see the Junos OS command references.

J-Web monitoring pages appear when you select **Monitor** in the taskbar. The monitoring pages display the current configuration on your system and the status of your system, chassis, interfaces, and routing and security operations. The monitoring pages have plus signs (+) that you can expand to view details. On some pages, such as the Routing Information page, you can specify search criteria to view selective information.

## Class of Service

To display details about the performance of class of service (CoS) on a Juniper device, select **Monitor>Class of Service** in the J-Web interface.

Table 72 on page 637 shows a summary of the information displayed on the Class of Service pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

**Table 72: Class of Service Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
<b>Interfaces</b>	
Information about the physical and logical interfaces in the system and details about the CoS components assigned to these interfaces.	<b>show class-of-service interface</b>
<b>Classifiers</b>	
Forwarding classes and loss priorities that incoming packets are assigned to based on the packet's CoS values.	<b>show class-of-service classifier</b>
<b>CoS Value Aliases</b>	
CoS value aliases that the system is using to represent DiffServ code point (DSCP), DSCP IPv6, MPLS experimental (EXP), and IPv4 precedence bits.	<b>show class-of-service code-point-aliases</b>
<b>RED Drop Profiles</b>	
Detailed information about the drop profiles used by the system. Also, displays a graph of the random early detection (RED) curve that the system uses to determine the queue fullness and drop probability.	<b>show class-of-service drop-profile</b>
<b>Forwarding Classes</b>	
Assignment of forwarding classes to queue numbers.	<b>show class-of-service forwarding-class</b>
<b>Rewrite Rules</b>	
Packet CoS value rewrite rules based on the forwarding classes and loss priorities.	<b>show class-of-service rewrite-rule</b>
<b>Scheduler Maps</b>	
Assignment of forwarding classes to schedulers. Schedulers include transmit rate, rate limit, and buffer size.	<b>show class-of-service scheduler-map</b>

## Interfaces

The J-Web interface hierarchically displays all Juniper device physical and logical interfaces, including state and configuration information. This information is divided into multiple parts. To view general interface information such as available interfaces, operation states of the interfaces, and descriptions of the configured interfaces, select **Monitor>Interfaces** in the J-Web interface. To view interface-specific properties such

as administrative state or traffic statistics in the J-Web interface, select the interface name on the Port Monitoring page and click **Details**. (See “[Sample Task—Monitoring Interfaces](#)” on page 645.)

[Table 73 on page 638](#) shows a summary of the information displayed on the Interfaces pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 73: Interfaces Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Status information about the specified Protocol Independent Multicast (PIM).	<b>show interfaces terse</b>
Detailed information about all interfaces configured on the Juniper device.	<b>show interfaces detail</b>
Current state of the interface you specify.	<b>show interfaces <i>interface-name</i></b>

## MPLS

To view information about MPLS label-switched paths (LSPs) and virtual private networks (VPNs), select **Monitor>MPLS**.

[Table 74 on page 638](#) shows a summary of the information displayed on the MPLS pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

**Table 74: MPLS Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
<b>Interfaces</b>	
Interfaces on which MPLS is enabled, plus the operational state and any administrative groups applied to an interface.	<b>show mpls interface</b>
<b>LSP Information</b>	
LSP sessions currently active on the Juniper device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	<b>show mpls lsp</b>
<b>LSP Statistics</b>	
Statistics for LSP sessions currently active on the Juniper device, including the total number of packets and bytes forwarded through an LSP.	<b>show mpls lsp statistics</b>
<b>RSVP Sessions</b>	
RSVP-signaled LSP sessions currently active on the Juniper device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	<b>show rsvp session</b>
<b>RSVP Interfaces</b>	

**Table 74: MPLS Information and the Corresponding CLI show Commands** (*continued*)

Information Displayed	Corresponding CLI Command
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.	<b>show rsvp interface</b>

## RPM

The real-time performance monitoring (RPM) information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the Juniper device. To view these RPM properties, select **Troubleshoot > RPM** in the J-Web interface.

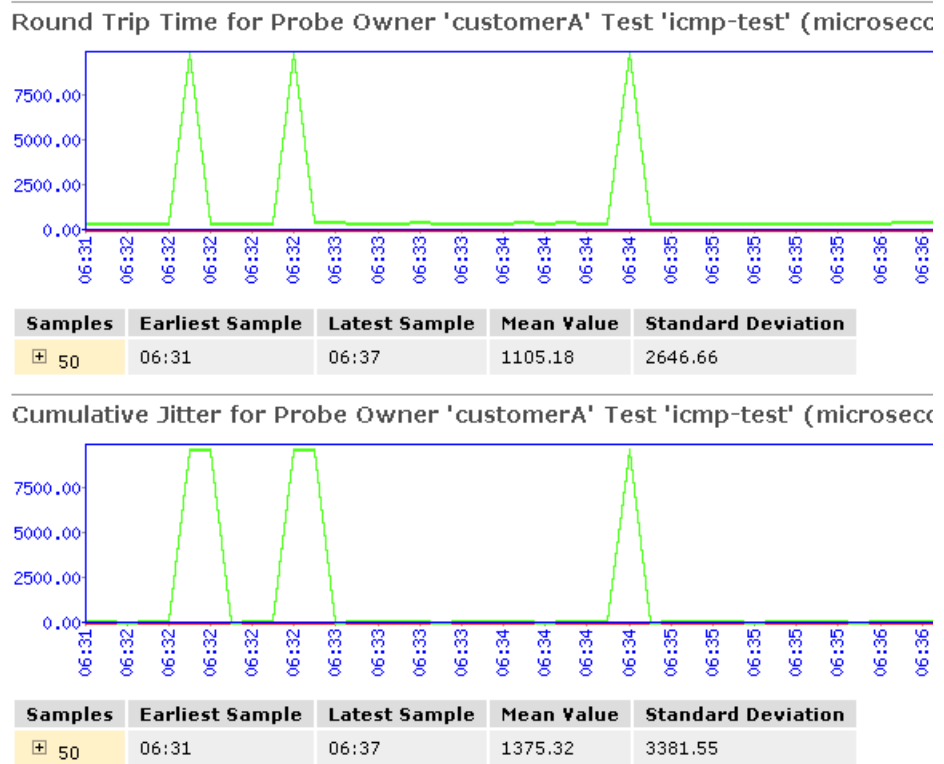
[Table 75 on page 639](#) shows a summary of the information displayed on the RPM page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

**Table 75: RPM Information and the Corresponding CLI show Command**

Information Displayed	Corresponding CLI Command
Results of the most recent RPM probes.	<b>show services rpm probe-results</b>

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. [Figure 45 on page 640](#) shows sample graphs for an RPM test.

Figure 45: Sample RPM Graphs



In [Figure 45 on page 640](#), 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.

## Routing

To view information about routes in a routing table or for information about OSPF, BGP, or RIP, select **Monitor>Routing** in the J-Web interface.

The routing information includes information about the route's destination, protocol, state, and parameters. To view selective information, type or select information in one or more of the Narrow Search boxes, and click **Search**.

[Table 76 on page 640](#) shows a summary of the information displayed on the Routing pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

**Table 76: Routing Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
<b>Route Information</b>	
A high-level summary of the routes in the routing table.	<b>show route terse</b>
Detailed information about the active entries in the routing tables.	<b>show route detail</b>

Table 76: Routing Information and the Corresponding CLI show Commands (*continued*)

Information Displayed	Corresponding CLI Command
<b>BGP Information</b>	
Summary about Border Gateway Protocol (BGP).	<b>show bgp summary</b>
BGP peers.	<b>show bgp neighbor</b>
<b>OSPF Information</b>	
Information about OSPF neighbors.	<b>show ospf neighbors</b>
OSPF interfaces.	<b>show ospf interfaces</b>
OSPF statistics.	<b>show ospf statistics</b>
<b>RIP Information</b>	
Routing Information Protocol (RIP) statistics about messages sent and received on an interface, as well as information received from advertisements from other routers.	<b>show rip statistics</b>
RIP neighbors.	<b>show rip neighbors</b>

Security

- [Firewall on page 641](#)
- [IPsec on page 642](#)
- [NAT on page 642](#)

Firewall

To view stateful firewall filter information in the J-Web interface, select **Monitor>Security>Firewall>Stateful Firewall**. To display stateful firewall filter information for a particular address prefix, port, or other characteristic, type information in or select information from one or more of the Narrow Search boxes, and click **OK**.

[Table 77 on page 642](#) shows a summary of the information displayed on Firewall pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 77: Firewall Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
<b>Statistics Summary</b>	
Stateful firewall filter statistics.	<b>show services stateful-firewall statistics</b>
<b>Stateful Firewall</b>	
Stateful firewall filter conversations.	<b>show services stateful-firewall conversations</b>
Flow table entries for stateful firewall filters.	<b>show services stateful-firewall flows</b>
<b>IDS Information</b>	
Information about an address under possible attack.	<b>show services ids destination-table</b>
Information about an address that is a suspected attacker.	<b>show services ids source-table</b>
Information about a particular suspected attack source-and-destination address pair.	<b>show services ids pair-table</b>

### IPsec

To view information about configured IP Security (IPsec) tunnels and statistics, and Internet Key Exchange (IKE) security associations for adaptive services interfaces, select **Monitor>Security>IPsec** in the J-Web interface.

[Table 78 on page 642](#) shows a summary of the information displayed on the IPsec page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 78: IPsec Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
(Adaptive services interface only) IPsec statistics for the selected service set.	<b>show services ipsec-vpn ipsec statistics</b>
(Adaptive services interface only) IPsec security associations for the selected service set.	<b>show services ipsec-vpn ipsec security-associations</b>
(Adaptive services interface only) Internet Key Exchange (IKE) security associations.	<b>show services ipsec-vpn ike security-associations</b>

### NAT

NAT pool information includes information about the address ranges configured within the pool on the Juniper device. To view NAT pool information, select **Monitor>Security>NAT** in the J-Web interface.

[Table 79 on page 643](#) shows a summary of the information displayed on the NAT page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.



Table 79: NAT Information and the Corresponding CLI show Command

Information Displayed	Corresponding CLI Command
Information about Network Address Translation (NAT) pools.	<b>show services nat pool</b>

## Service Sets

Service set information includes the services interfaces on the Juniper device, the number of services sets configured on the interfaces, and the total CPU used by the service sets. To view these service set properties, select **Monitor>Service Sets** in the J-Web interface.

A service set is a group of rules from a stateful firewall filter, Network Address Translation (NAT), intrusion detection service (IDS), or IP Security (IPsec) that you apply to a services interface. IDS, NAT, and stateful firewall filter service rules can be configured within the same service set. However, IPsec services are configured in a separate service set.

[Table 80 on page 643](#) shows a summary of the information displayed on Service Sets pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 80: Service Sets Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Service set summary information.	<b>show services service-sets summary</b>
Service set memory usage.	<b>show services service-sets memory-usage</b>

## Services

To view information about dynamic and static DHCP leases, conflicts, pools, and statistics, select **Monitor>Services>DHCP** in the J-Web interface.

[Table 81 on page 643](#) shows a summary of the information displayed on the DHCP page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 81: DHCP Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
DHCP server client binding information.	<b>show system services dhcp binding</b>
DHCP client-detected conflicts for IP addresses.	<b>show system services dhcp conflict</b>
DHCP server IP address pools.	<b>show system services dhcp pool</b>
DHCP server statistics.	<b>show system services dhcp statistics</b>

## System View

- [System Information on page 644](#)
- [Chassis Information on page 644](#)
- [Process Details on page 645](#)
- [FEB Redundancy \(M120 Routing Platforms Only\) on page 645](#)

### System Information

To view information about system properties such as the name and IP address of the Juniper device or the resource usage on the Routing Engine, select **Monitor>System View** in the J-Web interface.

[Table 82 on page 644](#) shows a summary of the information displayed on System pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 82: System Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Current time and information about how long the Juniper device, Juniper device software, and routing protocols have been running.	<b>show system uptime</b>
Information about users who are currently logged in to the Juniper device.	<b>show system users</b>
Statistics about the amount of free disk space in the Juniper device's file systems.	<b>show system storage</b>
Software processes running on the Juniper device.	<b>show system processes</b>

### Chassis Information

To view chassis properties on the Juniper device, select **Monitor>System View>Chassis Information** in the J-Web interface.

[Table 83 on page 644](#) shows a summary of the information displayed on the Chassis Information page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 83: Chassis Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Conditions that have been configured to trigger alarms.	<b>show chassis alarms</b>
Environmental information about the Juniper device chassis, including the temperature and information about the fans, power supplies, and Routing Engine.	<b>show chassis environment</b>
Status information about the installed FPCs and PICs.	<b>show chassis fpc</b>

**Table 83: Chassis Information and the Corresponding CLI show Commands** (*continued*)

Information Displayed	Corresponding CLI Command
List of all FPCs and PICs installed in the Juniper device chassis, including the hardware version level and serial number.	<b>show chassis hardware</b>

### Process Details

To view process details like process ID, CPU load, or memory utilization, select **Monitor>System View>Process Details** in the J-Web interface.

Table 84 on page 645 shows a summary of the information displayed on the Process Details page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 84: Process Details Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Software processes running on the router	<b>show processes extensive</b>

### FEB Redundancy (M120 Routing Platforms Only)

On M120 routers, Forwarding Engine Boards (FEBs) provide route lookup and forwarding functions from Flexible PIC Concentrators (FPCs) and compact Flexible PIC Concentrators (cFPCs). You can configure FEB redundancy groups to provide high availability for FEBs.

To view the status of FEBs and FEB redundancy groups, or connectivity between FPCs and FEBs, select **Monitor>System View>FEB Redundancy** in the J-Web interface.

Table 85 on page 645 shows a summary of the information displayed on the FEB Redundancy page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

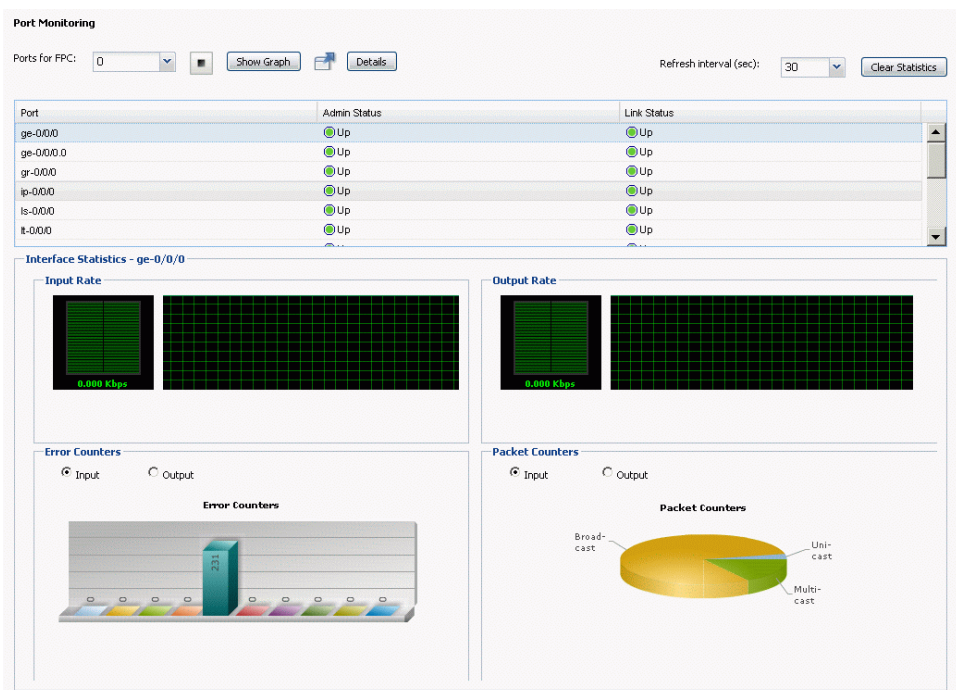
**Table 85: FEB Redundancy Information and the Corresponding CLI show Command**

Information Displayed	Corresponding CLI Command
Forwarding Engine Board (FEB) status information.	<b>show chassis feb</b>

### Sample Task—Monitoring Interfaces

Figure 46 on page 646 shows the Port Monitoring page that displays the interfaces installed on your Juniper device. At a glance, you can monitor the status of all the configured physical and logical interfaces.

Figure 46: Port Monitoring Page



You can select any interface and click **Details** to view details about its status. For example, selecting **ge-0/0/0** and clicking **Details**, displays detailed information about the interface (see [Figure 47 on page 647](#)).

Figure 47: Details of Interface ge-0/0/0 Page

Name	Value
name	ge-0/0/0
local-index	129
snmp-index	160
generation	132
link type	Ethernet
mtu	1514
source-filtering	disabled
link-mode	Full-duplex
speed	1000mbps
BPDU error	none
MAC-REWRITE Error	none
loopback	disabled
flow control	enabled
auto-negotiation	enabled
remote fault	online
device flags	present running
config flags	snmp-traps flags
media flags	none

OK

### Sample Task—Monitoring Route Information

Figure 48 on page 648 shows the Route Information monitoring page that displays information about all 9 routes in the routing table. All Juniper devices are active, and there are no hidden routes.

Figure 48: Monitoring Route Information Page with Complete Information

**Routing**

**Route Information**

9 destinations, 9 routes (8 active, 0 hold down, 1 hidden) Showing 8 of 9 routes

**inet.0**

Destination	Protocol/Preference	Next-Hop	Age
+ 0.0.0.0/0	*Static/5	Router	2w2d 19:46:24
+ 10.10.0.0/16	*Static/5	Router	2w2d 19:46:24
+ 10.209.0.0/18	*Direct/0	Interface	2w2d 19:46:24
+ 10.209.8.129/32	*Local/0	Local	2w2d 19:46:26
+ 172.16.0.0/12	*Static/5	Router	2w2d 19:46:24
+ 192.168.0.0/16	*Static/5	Router	2w2d 19:46:24
+ 192.168.102.0/23	*Static/5	Router	2w2d 19:46:24
+ 207.17.136.0/24	*Static/5	Router	2w2d 19:46:24

**Narrow Search**

Destination Address  Protocol

Next Hop Address  Receive Protocol

Best Route ☐ Inactive Routes ☐

Exact Route ☐ Hidden Routes ☐

Number of Routes to Display

By default, information about all routes in the routing table (up to a maximum of 25 routes on one page) is displayed. To view information about selective routes, type or select information in one or more of the Narrow Search boxes, and click **OK**. For example, typing **direct** in the box next to Protocol, displays the only 1 route. This is the only route that has **0** preference from a directly connected network. (see [Figure 49 on page 648](#)).

Figure 49: Monitoring Route Information Page with Selective Information

**Routing**

**Route Information**

9 destinations, 9 routes (8 active, 0 hold down, 1 hidden) Showing 1 of 9 routes

**inet.0**

Destination	Protocol/Preference	Next-Hop	Age
+ 10.209.0.0/18	*Direct/0	Interface	2w2d 22:01:22

**Narrow Search**

Destination Address  Protocol

Next Hop Address  Receive Protocol

Best Route ☐ Inactive Routes ☐

Exact Route ☐ Hidden Routes ☐

Number of Routes to Display

## Managing J-Web Sessions and Users

- [Setting J-Web Session Limits on page 649](#)
- [Terminating J-Web Sessions on page 649](#)
- [Viewing Current Users on page 649](#)

### Setting J-Web Session Limits

By default, an unlimited number of users can log in to the J-Web interface on a Juniper 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 Juniper 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 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 649](#).

### Viewing Current Users

To view a list of users logged in to the Juniper device, select **Monitor>System View>System Information** in J-Web and scroll down to the Logged-in User Details

section, or enter the **show system users** command in the CLI. The J-Web page and CLI output show all users logged in to the Juniper device from either J-Web or the CLI.



## CHAPTER 26

# Troubleshooting

- [Troubleshooting the J-Web User Interface on page 651](#)
- [Troubleshooting System Log Events on page 652](#)
- [Troubleshooting the Network on page 653](#)

### Troubleshooting the J-Web User Interface

---

- [Lost Router Connectivity on page 651](#)
- [Unpredictable J-Web Behavior on page 651](#)
- [No J-Web Access on page 652](#)

#### 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 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 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 an M Series or T Series router, 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 603](#).

**Solution 2**—If the Juniper 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 Juniper device.

## Troubleshooting System Log Events

- [Troubleshooting Events on page 652](#)

### Troubleshooting Events

**Problem**    **Description:** My View Events page does not display any events. (See [Figure 50 on page 652](#).)

**Figure 50: View Events Page Displaying Error**

The screenshot shows the 'View Events' interface. The 'Events Filter' section includes a 'System Log File' dropdown set to 'messages', an unchecked 'Include archived files' checkbox, 'Date From' and 'To' date pickers both set to '2009-07-17,03:54', and empty 'Event ID' and 'Description' input fields. There are 'Search' and 'Reset' buttons. Below the filter section is the 'Events Detail' table, which is currently empty with the message 'No events match filter condition'. A 'Generate Report' button is located at the top right of the table area.

Process	Severity	Event ID	Event Description	Time
No events match filter condition				

**Cause**    Typically, events are not displayed when logging of messages is not enabled. You can enable system log messages at a number of different levels using the J-Web configuration editor or the CLI terminal. The choice of level depends on how specific you want the event logging to be and what options you want to include. For details about the configuration options, see the *System Log Monitoring and Troubleshooting Guide for Security Devices*.

**Solution**    To enable system log messages with the J-Web configuration editor:

1. Navigate to **Configuration>View and Edit>Edit Configuration**.
2. Next to System, click **Configure** or **Edit** to navigate to the system level in the configuration hierarchy.
3. Next to Syslog, click **Configure** or **Edit** to navigate to the system log level in the configuration hierarchy.

4. Next to File, click **Add new entry** to create a log file.
5. In the File name box, type **messages** to name the log file.
6. Next to Contents, click **Add new entry** to select a facility that you want to configure—for example, **authorization**, **change-log**, **conflict-log**, or **user**.
7. In the Facility list, select **authorization** to configure the authorization facility.
8. In the Level list, select **info** to set the severity level to informational messages.
9. Repeat Steps 4 and 5 to configure different facilities and their levels.
10. To verify the configuration, at the CLI terminal, enter the **show syslog** command in configuration mode. (See [Figure 51 on page 653](#).)

**Figure 51: Verifying System Log Messages Configuration**

```

CLI Terminal

A Java applet will be loaded below that will provide an SSH connection between your browser and '10.204.92.13'. You will be asked to enter your password again as a security
measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or
you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

--- JUNOS 9.3R2.8 built 2008-12-17 23:25:33 UTC
% cli
regress@jotter> configure
Entering configuration mode

[edit]
regress@jotter# edit system

[edit system]
regress@jotter# show syslog
file messages {
 any notice;
 authorization info;
 kernel info;
 pfe info;
 archive world-readable;
}

[edit system]
regress@jotter#

```

## Troubleshooting the Network

- [Using Ping Host on page 653](#)
- [Using Ping MPLS on page 654](#)
- [Using Traceroute on page 656](#)
- [Using Packet Capture on page 656](#)
- [Sample Task—Ping Host on page 657](#)

### Using Ping Host

Use the Ping Host page to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The Juniper device sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to a specified host to determine:

- Whether a remote host is active or inactive
- The round-trip delay in communicating with the host
- Packet loss

Entering a hostname or address on the Ping Host page creates a periodic ping task that runs until canceled or until it times out as specified. When you use the ping host tool, the Juniper device first sends an echo request packet to an address, then waits for a reply. The ping is successful if it has the following results:

- The echo request gets to the destination host.
- The destination host is able to get an echo reply back to the source within a predetermined time called the round-trip time.

Alternatively, you can enter the **ping** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 599](#). For more information about the **ping** command, see [CLI Explorer](#).

Because some hosts are configured not to respond to ICMP echo requests, a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you might find that you are not able to ping outside your local network.

## Using Ping MPLS

Use the Ping MPLS page to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits. You can ping an MPLS endpoint using various options. You can send variations of ICMP echo request packets to the specified MPLS endpoint.

When you use the ping MPLS task from a Junos OS operating as the inbound (ingress) node at the entry point of an LSP or VPN, the Juniper device sends probe packets into the LSP or VPN. 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 Junos OS receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

[Table 86 on page 655](#) lists the ping MPLS tasks, summarizes their functions, and identifies corresponding CLI **show** commands you can enter at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 599](#).

Table 86: Ping MPLS Tasks Summary and the Corresponding CLI show Commands

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
<b>Ping RSVP-signaled LSP</b>	<b>ping mpls rsvp</b>	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The Junos OS pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the Junos OS sends the ping requests on the path that is currently active.
<b>Ping LDP-signaled LSP</b>	<b>ping mpls ldp</b>	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The Junos OS pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the Junos OS sends the ping requests through the first gateway.  Ping requests sent to LDP-signaled LSPs use only the master routing instance.
<b>Ping LSP to Layer 3 VPN prefix</b>	<b>ping mpls l3vpn</b>	Checks the operability of the connections related to a Layer 3 VPN. The Junos OS tests whether a prefix is present in a provider edge (PE) router's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix.	The Junos OS does not test the connection between a PE router and a customer edge (CE) router.
<b>Ping LSP for a Layer 2 VPN connection by interface</b>	<b>ping mpls l2vpn interface</b>	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS directs outgoing request probes out the specified interface.	For information about interface names, see the <i>Interfaces Feature Guide for Security Devices</i> .
<b>Ping LSP for a Layer 2 VPN connection by instance</b>	<b>ping mpls l2vpn instance</b>	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS 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.	
<b>Ping LSP to a Layer 2 circuit remote site by interface</b>	<b>ping mpls l2circuit interface</b>	Checks the operability of the Layer 2 circuit connections. The Junos OS directs outgoing request probes out the specified interface.	
<b>Ping LSP to a Layer 2 circuit remote site by VCI</b>	<b>ping mpls l2circuit virtual-circuit</b>	Checks the operability of the Layer 2 circuit connections. The Junos OS 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 86: Ping MPLS Tasks Summary and the Corresponding CLI show Commands (*continued*)

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping end point of LSP	<code>ping mpls lsp-end-point</code>	Checks the operability of an LSP endpoint. The Junos OS pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address.	

## Using Traceroute

Use the Traceroute page to trace a route between the Juniper device and a remote host. You can use the traceroute task to display a list of routers between the Juniper device and a specified destination host. The output is useful for diagnosing a point of failure in the path from the Juniper device to the destination host, and addressing network traffic latency and throughput problems.

The Juniper device generates the list of routers by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive router is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each router along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The Juniper device sends a total of three traceroute packets to each router along the path and displays the round-trip time for each traceroute operation. If the Juniper device times out before receiving a **Time Exceeded** message, an asterisk (\*) is displayed for that round-trip time.

Alternatively, you can enter the **traceroute** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 599](#). For more information about the **traceroute** command, see [CLI Explorer](#).

## Using Packet Capture

Use the Packet Capture page when you need to quickly capture and analyze router control traffic on a Juniper device. The Packet Capture page allows you to capture traffic destined for or originating from the Routing Engine. You can use the packet capture task 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 interface as they are captured, or save the captured packets to a file and analyze them offline with packet analyzers such as Ethereal. The packet capture task does not capture transient traffic.

Alternatively, you can use the CLI **monitor traffic** command at the J-Web CLI terminal to capture and display packets matching a specific criteria. For more information, see [“Using the CLI Terminal” on page 599](#). For more information about the **monitor traffic** command, see [CLI Explorer](#).

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web or CLI configuration editor. .

## Sample Task—Ping Host

Figure 52 on page 657 shows a sample Ping Host page. In this example, you are sending ping requests to two destination hosts—10.10.2.2 and 10.10.10.10. The echo requests reaches 10.10.2.2 and does not reach 10.10.10.10.

To ping the host:

1. Select **Troubleshoot>Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 52 on page 657).
3. Next to Remote Host, type 10.10.2.2 to specify the host's IP address.
4. Retain the default values in the following fields:
  - Interface—**any**—Ping requests to be sent on all interfaces.
  - Count—**10**—Number of ping requests to send.
  - Type-of-Service—**0**—TOS value in the IP header of the ping request packet.
  - Routing Instance—**default**—Routing instance name for the ping attempt.
  - Interval—**1**—Interval, in seconds, between the transmission of each ping request.
  - Packet Size—**56**—Size of the ping request packet in bytes. The Juniper device adds 8 bytes of ICMP header to this size before sending it.
  - Time-to-Live—**32**—TTL hop count for the ping request packet.
5. Click **Start**.
6. Repeat Steps 2 through 5 to ping destination host 10.10.10.10.

Figure 52: Ping Host Troubleshoot Page

**Ping Host**

---

**Ping Host**

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

Entering a host below creates a periodic ping task that will run until cancelled or until it times out as specified.

\* Remote Host  ?

**Advanced options**

Don't Resolve Addresses <input type="checkbox"/> ? Interface <input type="text" value="any"/> ? Count <input type="text" value="10"/> ? Don't Fragment <input type="checkbox"/> ? Record Route <input type="checkbox"/> ? Type-of-Service <input type="text" value="0"/> ?	Routing Instance <input type="text" value="default"/> ? Interval <input type="text" value="1"/> ? Packet Size <input type="text" value="56"/> ? Source Address <input type="text"/> ? Time-to-Live <input type="text" value="32"/> ? Bypass Routing <input type="checkbox"/> ?
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Start**

Figure 53 on page 658 displays the results of a successful ping in the main pane, and Table 87 on page 658 provides a summary of the ping host results and output.

Figure 53: Successful Ping Host Results Page

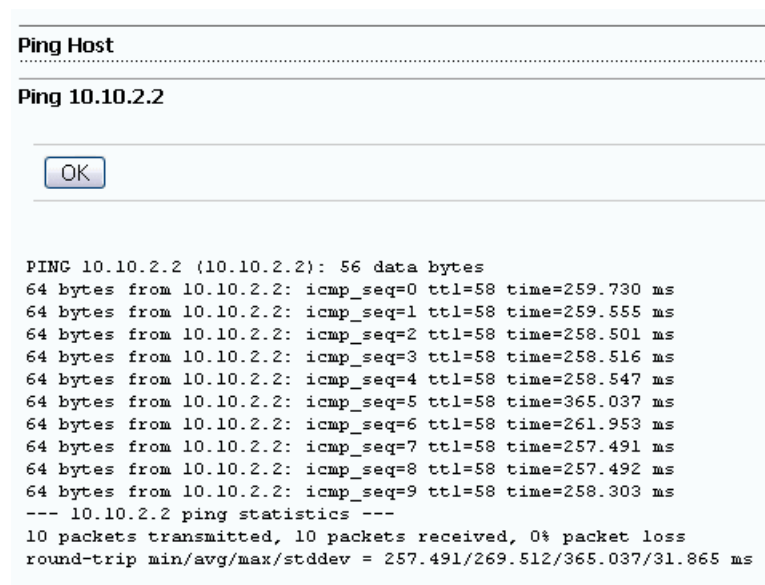


Table 87: J-Web Ping Host Results and Output Summary

Ping Host Result	Description
64 bytes from	Size of ping response packet, which is equal to the default value in the Packet Size box (56), plus 8.
10.10.2.2	IP address of the destination host that sent the ping response packet.
icmp_seq= <i>number</i>	Sequence numbers of packets from 0 through 9. You can use this value to match the ping response to the corresponding ping request.
ttl=58	Time-to-live hop-count value of the ping response packet.
259.730 ms	Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
10 packets transmitted, 10 packets received, 0% packet loss	Ping packets transmitted, received, and lost. 10 ping requests (probes) were sent to the host, and 10 ping responses were received from the host. No packets were lost.
257.491/269.512/365.037/31.865 ms	<ul style="list-style-type: none"> <li>257.491—Minimum round-trip time</li> <li>269.512—Average round-trip time</li> <li>365.037—Maximum round-trip time</li> <li>31.865—Standard deviation of the round-trip times</li> <li>ms—milliseconds</li> </ul>



Figure 54 on page 659 shows the output of an unsuccessful ping. There can be different reasons for an unsuccessful ping. This result shows that the local router did not have a route to the host 10.10.10.10 and thus could not reach it.

Figure 54: Unsuccessful Ping Host Results Page

#### Ping Host

#### Ping 10.10.10.10

OK

```

PING 10.10.10.10 (10.10.10.10): 56 data bytes
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 3825 0 0000 1a 01 411f 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 383e 0 0000 1a 01 4106 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 384f 0 0000 1a 01 40f5 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable

```



## PART 5

# Administration Guide for Security Devices

- [User Access and Authentication on page 663](#)
- [Configuring Remote Access to an SRX Series Appliances on page 865](#)
- [Configuring DNS on page 905](#)
- [Configuring DHCP Access Service for IP Address Management on page 917](#)
- [Managing System Files on page 977](#)
- [Working with Junos OS Licenses on page 989](#)
- [Configuration Statements and Operational Commands on page 1009](#)



## CHAPTER 27

# User Access and Authentication

- [User Access and Authentication Overview on page 663](#)
- [Configuring Junos OS User Accounts on page 674](#)
- [Configuring User Access Privileges on page 694](#)
- [Permissions Flags for User Access Privileges on page 702](#)
- [Configuring Authentication Methods on page 851](#)

## User Access and Authentication Overview

---

- [Understanding Login Classes on page 663](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Understanding User Authentication Methods on page 673](#)

## Understanding Login Classes

All users who log into 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 into 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 88 on page 663](#) contains a few predefined login classes. The predefined login classes cannot be modified.

**Table 88: Predefined Login Classes**

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view

Table 88: Predefined Login Classes (*continued*)

Login Class	Permission Bits Set
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 664](#)
- [Denying or Allowing Individual Commands on page 666](#)

### 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 89 on page 664](#)).

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 89: Permission Bits for Login Classes

Permission Bit	Access
admin	Can view user account information in configuration mode and with the <b>show configuration</b> command.
admin-control	Can view user accounts and configure them (at the <b>[edit system login]</b> hierarchy level).

Table 89: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
<b>access</b>	Can view the access configuration in configuration mode and with the <b>show configuration</b> operational mode command.
<b>access-control</b>	Can view and configure access information (at the <b>[edit access]</b> hierarchy level).
<b>all</b>	Has all permissions.
<b>clear</b>	Can clear (delete) information learned from the network that is stored in various network databases (using the <b>clear</b> commands).
<b>configure</b>	Can enter configuration mode (using the <b>configure</b> command) and commit configurations (using the <b>commit</b> command).
<b>control</b>	Can perform all control-level operations (all operations configured with the <b>-control</b> permission bits).
<b>field</b>	Reserved for field (debugging) support.
<b>firewall</b>	Can view the firewall filter configuration in configuration mode.
<b>firewall-control</b>	Can view and configure firewall filter information (at the <b>[edit firewall]</b> hierarchy level).
<b>floppy</b>	Can read from and write to the removable media.
<b>interface</b>	Can view the interface configuration in configuration mode and with the <b>show configuration</b> operational mode command.
<b>interface-control</b>	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 <b>[edit]</b> hierarchy).
<b>maintenance</b>	Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the <b>su root</b> command), and can halt and reboot the device (using the <b>request system</b> commands).
<b>network</b>	Can access the network by entering the <b>ping</b> , <b>ssh</b> , <b>telnet</b> , and <b>traceroute</b> commands.
<b>reset</b>	Can restart software processes using the <b>restart</b> command and can configure whether software processes are enabled or disabled (at the <b>[edit system processes]</b> hierarchy level).
<b>rollback</b>	Can use the <b>rollback</b> command to return to a previously committed configuration other than the most recently committed one.
<b>routing</b>	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.

Table 89: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
<b>routing-control</b>	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the <b>[edit routing-options]</b> hierarchy level), routing protocols (at the <b>[edit protocols]</b> hierarchy level), and routing policy (at the <b>[edit policy-options]</b> hierarchy level).
<b>secret</b>	Can view passwords and other authentication keys in the configuration.
<b>secret-control</b>	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
<b>security</b>	Can view security configuration in configuration mode and with the <b>show configuration</b> operational mode command.
<b>security-control</b>	Can view and configure security information (at the <b>[edit security]</b> hierarchy level).
<b>shell</b>	Can start a local shell on the device by entering the <b>start shell</b> command.
<b>snmp</b>	Can view SNMP configuration information in configuration and operational modes.
<b>snmp-control</b>	Can view SNMP configuration information and configure SNMP (at the <b>[edit snmp]</b> hierarchy level).
<b>system</b>	Can view system-level information in configuration and operational modes.
<b>system-control</b>	Can view system-level configuration information and configure it (at the <b>[edit system]</b> hierarchy level).
<b>trace</b>	Can view trace file settings in configuration and operational modes.
<b>trace-control</b>	Can view trace file settings and configure trace file properties.
<b>view</b>	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 673](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Template Accounts on page 677](#)
- [Example: Configuring New Users on page 674](#)



## 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 account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user. 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. The username can be up to 64 characters long.
- **User's full name**—(Optional) If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- **User identifier (UID)**—(Optional) 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.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- **User's access privilege**—(Required) 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—(Optional) 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.

```
[edit system login user username]
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long.
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Valid passwords must contain at least one change of case or character class.

Junos-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria 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.

For SSH authentication, you can copy the contents of an SSH key file into the configuration or directly configure SSH key information. Use the **load-key-file** *URL filename* command to load an SSH key file that was previously generated, e.g. by using **ssh-keygen**. The *URL filename* is the path to the file's location and name. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you enter the **load-key-file** statement. Optionally, you can use the **ssh-dsa public key <from hostname>** and the **ssh-rsa public key <from hostname>** statements to directly configure SSH keys.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them.

To view the SSH keys entries, use the configuration mode **show** command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host:.ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
 ssh-rsa "1024 35 9727638204084251055468226757249864241630322
207404962528390382038690141584534964170019610608358722961563
475784918273603361276441874265946893207739108344813125957722
625461667999278316123500438660915866283822489746732605661192
181489539813862940327687806538169602027491641637359132693963
44008443 user@example.net"; # SECRET-DATA
}
```

An account for the user **root** is always present in the configuration. You configure the password for **root** using the root-authentication statement.

#### Related Documentation

- [Understanding User Authentication Methods on page 673](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 855](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 859](#)
- [Example: Configuring Authentication Order on page 862](#)

## 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 669](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 672](#)

### Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in [Table 90 on page 669](#). 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 90 on page 669](#) 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 90: Login Class Permission Flags**

Permission Flag	Description
<b>access</b>	Can view the access configuration in configuration mode and with the <b>show configuration</b> operational mode command.
<b>access-control</b>	Can view and configure access information at the <b>[edit access]</b> hierarchy level.
<b>admin</b>	Can view user account information in configuration mode and with the <b>show configuration</b> operational mode command.
<b>admin-control</b>	Can view user accounts and configure them at the <b>[edit system login]</b> hierarchy level.

Table 90: Login Class Permission Flags (*continued*)

Permission Flag	Description
<b>all-control</b>	Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.
<b>clear</b>	Can clear (delete) information learned from the network that is stored in various network databases by using the <b>clear</b> commands.
<b>configure</b>	Can enter configuration mode by using the <b>configure</b> command.
<b>control</b>	Can perform all control-level operations—all operations configured with the <b>-control</b> permission flags.
<b>field</b>	Can view field debug commands. Reserved for debugging support.
<b>firewall</b>	Can view the firewall filter configuration in configuration mode.
<b>firewall-control</b>	Can view and configure firewall filter information at the <b>[edit firewall]</b> hierarchy level.
<b>floppy</b>	Can read from and write to the removable media.
<b>flow-tap</b>	Can view the flow-tap configuration in configuration mode.
<b>flow-tap-control</b>	Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the <b>[edit services flow-tap]</b> hierarchy level.
<b>flow-tap-operation</b>	<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 <b>flow-tap-operation</b> permission.</p> <p><b>NOTE:</b> The <b>flow-tap-operation</b> option is not included in the <b>all-control</b> permissions flag.</p>
<b>idp-profiler-operation</b>	Can view profiler data.
<b>interface</b>	Can view the interface configuration in configuration mode and with the <b>show configuration</b> operational mode command.

Table 90: Login Class Permission Flags (*continued*)

Permission Flag	Description
<b>interface-control</b>	Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: <ul style="list-style-type: none"> <li>• <b>[edit chassis]</b></li> <li>• <b>[edit class-of-service]</b></li> <li>• <b>[edit groups]</b></li> <li>• <b>[edit forwarding-options]</b></li> <li>• <b>[edit interfaces]</b></li> </ul>
<b>maintenance</b>	Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the <b>su root</b> command, and can halt and reboot the router or switch by using the <b>request system</b> commands.
<b>network</b>	Can access the network by using the <b>ping</b> , <b>ssh</b> , <b>telnet</b> , and <b>traceroute</b> commands.
<b>pgcp-session-mirroring</b>	Can view the <b>pgcp</b> session mirroring configuration.
<b>pgcp-session-mirroring-control</b>	Can modify the <b>pgcp</b> session mirroring configuration.
<b>reset</b>	Can restart software processes by using the <b>restart</b> command and can configure whether software processes are enabled or disabled at the <b>[edit system processes]</b> hierarchy level.
<b>rollback</b>	Can use the <b>rollback</b> command to return to a previously committed configuration other than the most recently committed one.
<b>routing</b>	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
<b>routing-control</b>	Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the <b>[edit routing-options]</b> hierarchy level, routing protocols at the <b>[edit protocols]</b> hierarchy level, and routing policy at the <b>[edit policy-options]</b> hierarchy level.
<b>secret</b>	Can view passwords and other authentication keys in the configuration.
<b>secret-control</b>	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
<b>security</b>	Can view security configuration in configuration mode and with the <b>show configuration</b> operational mode command.

Table 90: Login Class Permission Flags (*continued*)

Permission Flag	Description
<b>security-control</b>	Can view and configure security information at the <b>[edit security]</b> hierarchy level.
<b>shell</b>	Can start a local shell on the router or switch by using the <b>start shell</b> command.
<b>snmp</b>	Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.
<b>snmp-control</b>	Can view SNMP configuration information and can modify SNMP configuration at the <b>[edit snmp]</b> hierarchy level.
<b>system</b>	Can view system-level information in configuration and operational modes.
<b>system-control</b>	Can view system-level configuration information and configure it at the <b>[edit system]</b> hierarchy level.
<b>trace</b>	Can view trace file settings and configure trace file properties.
<b>trace-control</b>	Can modify trace file settings and configure trace file properties.
<b>view</b>	Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.
<b>view-configuration</b>	Can view all of the configuration excluding secrets, system scripts, and event options.  <b>NOTE:</b> Only users with the <b>maintenance</b> permission can view commit script, op script, or event script configuration.

### 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.

- 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 694](#)

## 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 into 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 667](#)
- [Understanding Login Classes on page 663](#)
- [Understanding Template Accounts on page 677](#)
- [Example: Configuring Authentication Order on page 862](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 855](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 859](#)

---

## Configuring Junos OS User Accounts

---

- [Example: Configuring New Users on page 674](#)
- [Understanding Template Accounts on page 677](#)
- [Example: Creating Template Accounts on page 677](#)
- [Understanding Administrative Roles on page 680](#)
- [Example: Configuring Administrative Roles on page 682](#)
- [Handling Authorization Failure on page 689](#)
- [Example: Configuring System Retry Options on page 690](#)

### Example: Configuring New Users

This example shows how to configure new users.

- [Requirements on page 674](#)
- [Overview on page 674](#)
- [Configuration on page 675](#)
- [Verification on page 677](#)

---

#### 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, and then 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
1ABC123
```

#### 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* 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
1ABC123
```

**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 "1ABC123";
 }
}
```

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 855](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 859](#).
- Configure a user. See [“Example: Configuring New Users” on page 674](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 677](#).

### 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 673](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Template Accounts on page 677](#)
- [Understanding Login Classes on page 663](#)

## 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 673](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Login Classes on page 663](#)
- [Example: Creating Template Accounts on page 677](#)

## Example: Creating Template Accounts

This example shows how to create template accounts.

- [Requirements on page 678](#)
- [Overview on page 678](#)
- [Configuration on page 678](#)
- [Verification on page 680](#)

## 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 678](#)
- [Creating a Local Template Account on page 679](#)

### ***Creating a Remote Template Account***

**CLI Quick Configuration** To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
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* 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 section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
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* 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 855.](#)
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 859.](#)
- Configure system authentication order. See [“Example: Configuring Authentication Order” on page 862.](#)

### 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 673](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Login Classes on page 663](#)
- [Understanding Template Accounts on page 677](#)

## 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 682](#)

## 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 683](#)
- [Overview on page 683](#)
- [Configuration on page 683](#)
- [Verification on page 688](#)



## 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, and then 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*.

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 "1ABC123"; ## SECRET-DATA
 }
 }
}

```

```

 }
 }
 user crypto-officer {
 class crypto-admin;
 authentication {
 encrypted-password "1ABC123"; ## SECRET-DATA
 }
 }
 user security-officer {
 class security-admin;
 authentication {
 encrypted-password "1ABC123"; ##SECRET-DATA
 }
 }
 user ids-officer {
 class ids-admin;
 authentication {
 encrypted-password "1ABC123"; ## 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: 'netscreen' 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
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 680](#)

## 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 system **message** defines the system login message. This message appears before a user logs in.

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.



**NOTE:** To clear the console during an administrator- initiated logout, the administrator must configure the set system login message “message string” such that, the message-string contains newline (\n) characters and a login banner message at the end of the \n characters.

To ensure that configuration information is cleared completely, the administrator can enter 50 or more `\n` characters in the *message-string* of the command `set system login message "message string"`.

For example, set system login message

"~~~~~  
Welcome to Junos!!!"

## Related Documentation

- [Example: Configuring System Retry Options on page 690](#)

### Example: Configuring System Retry Options

This example shows how to configure system retry options to protect the device from malicious users.

- Requirements on page 690
- Overview on page 690
- Configuration on page 693
- Verification on page 694

## Requirements

Before you begin, you should understand “[Handling Authorization Failure](#)” on page 689.

No special configuration beyond device initialization is required before configuring this feature.

## Overview

Malicious users sometimes try to log in to a secure device by guessing an authorized user account's password. Locking out a user account after a number of failed authentication attempts helps protect the device from malicious users.



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 the lockout-period, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
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** 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* in the *CLI User Guide*.

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;
```

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 3 unsuccessful logins for a particular username. The device gets locked for the user and then login to the device with a different user name. From operational mode, enter the **show system login lockout** command.

**Meaning** When you perform 3 unsuccessful login attempts with a particular username, the device is locked for that user for 5 minutes as configured in the example. You can verify that the user is, locked 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 689](#)

## Configuring User Access Privileges

---

- [Configuring Access Privilege Levels on page 694](#)
- [Example: Configuring Access Privilege Levels on page 695](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Example: Configuring Access Privileges for Operational Mode Commands on page 697](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 698](#)

## 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 Access Privilege Levels on page 695](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Junos OS Login Classes Overview](#)

## Example: Configuring 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:

```
[edit]
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 694](#)

## 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";
```

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 Access Privileges for Operational Mode Commands on page 697](#)

## Example: Configuring Access Privileges for Operational Mode Commands

The following example shows how to configure access privileges for different login classes for individual operational mode commands:

```
[edit]
system {
 # This login class has operator privileges and the additional ability
 # to reboot the router.
 login {
 # This login class has operator privileges and the additional ability to reboot the
 # router or switch.
 class operator-and-boot {
 permissions [clear network reset trace view];
 allow-commands "request system reboot";
 }
 # This login class has operator privileges but can't use any commands beginning
 # with "set" .
 # This login class has operator privileges
 # but cannot use any commands beginning with "set"
 class operator-no-set {
 permissions [clear network reset trace view];
 deny-commands "^set";
 }
 # This login class has operator privileges and can install software but not view
 # BGP information, and can issue the show route command, without specifying
 # commands or arguments under it.
 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 695](#)

## 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 695](#)
- [Example: Configuring Access Privilege Levels on page 695](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)

### 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 698](#)
- [Overview on page 698](#)
- [Configuration on page 699](#)
- [Examples Using Allow or Deny Configurations with Regular Expressions on page 699](#)

---

#### 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 695](#)
- [Example: Configuring Access Privilege Levels on page 695](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)

---

## Permissions Flags for User Access Privileges

---

- [Access Privilege User Permission Flags Overview on page 703](#)
- [access on page 705](#)
- [access-control on page 706](#)
- [admin on page 706](#)
- [admin-control on page 707](#)
- [all-control on page 708](#)
- [clear on page 708](#)
- [configure on page 742](#)
- [control on page 742](#)
- [field on page 742](#)
- [firewall on page 743](#)
- [firewall-control on page 743](#)
- [floppy on page 744](#)
- [flow-tap on page 744](#)
- [flow-tap-control on page 745](#)
- [flow-tap-operation on page 745](#)
- [idp-profiler-operation on page 746](#)
- [interface on page 746](#)
- [interface-control on page 747](#)

- [maintenance on page 748](#)
- [network on page 754](#)
- [pgcp-session-mirroring on page 755](#)
- [pgcp-session-mirroring-control on page 756](#)
- [reset on page 756](#)
- [rollback on page 757](#)
- [routing on page 757](#)
- [routing-control on page 761](#)
- [secret on page 765](#)
- [secret-control on page 766](#)
- [security on page 767](#)
- [security-control on page 771](#)
- [shell on page 774](#)
- [snmp on page 774](#)
- [system on page 775](#)
- [system-control on page 777](#)
- [trace on page 778](#)
- [trace-control on page 783](#)
- [view on page 788](#)
- [view-configuration on page 851](#)

## 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 669](#)
- [access on page 705](#)
- [access-control on page 706](#)
- [admin on page 706](#)
- [admin-control on page 707](#)
- [all-control on page 708](#)
- [clear on page 708](#)
- [configure on page 742](#)
- [control on page 742](#)
- [field on page 742](#)
- [firewall on page 743](#)
- [firewall-control on page 743](#)
- [floppy on page 744](#)
- [flow-tap on page 744](#)
- [flow-tap-operation on page 745](#)
- [idp-profiler-operation on page 746](#)
- [interface on page 746](#)
- [interface-control on page 747](#)
- [maintenance on page 748](#)
- [network on page 754](#)
- [pgcp-session-mirroring on page 755](#)
- [pgcp-session-mirroring-control on page 756](#)
- [reset on page 756](#)
- [rollback on page 757](#)
- [routing on page 757](#)
- [routing-control on page 761](#)
- [secret on page 765](#)
- [secret-control on page 766](#)
- [security on page 767](#)

- [security-control on page 771](#)
- [shell on page 774](#)
- [snmp on page 774](#)
- [system on page 775](#)
- [system-control on page 777](#)
- [trace on page 778](#)
- [trace-control on page 783](#)
- [view on page 788](#)
- [view-configuration on page 851](#)

## access

Can view the access configuration in configuration mode.

**Commands** No associated CLI commands.

### 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [access-control on page 706](#)

## 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [access on page 705](#)

## admin

Can view user account information in configuration mode.

### 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 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]  
 [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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [admin-control on page 707](#)

## 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [admin on page 706](#)

## 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**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## clear

Can clear (delete) information learned from the network that is stored in various network databases.

**Commands**

```
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 subscriber
<clear-ancp-subscriber-connection>
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
<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 mac-table
<clear-bridge-mac-table>
clear bridge mac-table interface
<clear-bridge-interface-mac-table>
clear appqos-counter
clear appqos-rate-limiter-statistics
clear appqos-rule-statistics
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 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-arp-aggregate-states>
```

```
clear ddos-protection protocols arp aggregate statistics
clear-ddos-arp-aggregate-statistics
clear ddos-protection protocols arp states
clear-ddos-arp-states
clear ddos-protection protocols arp statistics
clear-ddos-arp-statistics
clear ddos-protection protocols atm
clear ddos-protection protocols atm aggregate
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 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 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 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 states
clear-ddos-bgp-aggregate-states
clear ddos-protection protocols bgp aggregate statistics
clear-ddos-bgp-aggregate-statistics
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 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-bgpv6-states
clear ddos-protection protocols bgpv6 statistics
clear-ddos-bgpv6-statistics
```

```
clear ddos-protection protocols demux-autosense
clear ddos-protection protocols demux-autosense aggregate
clear ddos-protection protocols demux-autosense aggregate states
clear-ddos-demuxauto-aggregate-states
clear ddos-protection protocols demux-autosense aggregate statistics
clear-ddos-demuxauto-aggregate-statistics
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 states
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 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 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 states
clear-ddos-dhcpv4-inform-states
clear ddos-protection protocols dhcpv4 inform statistics
clear-ddos-dhcpv4-inform-statistics
clear ddos-protection protocols dhcpv4 lease-active
clear ddos-protection protocols dhcpv4 lease-active states
clear-ddos-dhcpv4-leaseact-states
clear ddos-protection protocols dhcpv4 lease-active statistics
clear-ddos-dhcpv4-leaseact-statistics
```

```
clear ddos-protection protocols dhcpv4 lease-query
clear ddos-protection protocols dhcpv4 lease-query states
clear-ddos-dhcpv4-leasequery-states
clear ddos-protection protocols dhcpv4 lease-query statistics
clear-ddos-dhcpv4-leasequery-statistics
clear ddos-protection protocols dhcpv4 lease-unassigned
clear ddos-protection protocols dhcpv4 lease-unassigned states
clear-ddos-dhcpv4-leaseuna-states
clear ddos-protection protocols dhcpv4 lease-unassigned statistics
clear-ddos-dhcpv4-leaseuna-statistics
clear ddos-protection protocols dhcpv4 lease-unknown
clear ddos-protection protocols dhcpv4 lease-unknown states
clear-ddos-dhcpv4-leaseunk-states
clear ddos-protection protocols dhcpv4 lease-unknown statistics
clear-ddos-dhcpv4-leaseunk-statistics
clear ddos-protection protocols dhcpv4 nak
clear ddos-protection protocols dhcpv4 nak states
clear-ddos-dhcpv4-nak-states
clear ddos-protection protocols dhcpv4 nak statistics
clear-ddos-dhcpv4-nak-statistics
clear ddos-protection protocols dhcpv4 no-message-type
clear ddos-protection protocols dhcpv4 no-message-type states
clear-ddos-dhcpv4-no-msgtype-states
clear ddos-protection protocols dhcpv4 no-message-type statistics
clear-ddos-dhcpv4-no-msgtype-statistics
clear ddos-protection protocols dhcpv4 offer
clear ddos-protection protocols dhcpv4 offer states
clear-ddos-dhcpv4-offer-states
clear ddos-protection protocols dhcpv4 offer statistics
clear-ddos-dhcpv4-offer-statistics
clear ddos-protection protocols dhcpv4 release
clear ddos-protection protocols dhcpv4 release states
clear-ddos-dhcpv4-release-states
clear ddos-protection protocols dhcpv4 release statistics
clear-ddos-dhcpv4-release-statistics
clear ddos-protection protocols dhcpv4 renew
clear ddos-protection protocols dhcpv4 renew states
clear-ddos-dhcpv4-renew-states
clear ddos-protection protocols dhcpv4 renew statistics
clear-ddos-dhcpv4-renew-statistics
clear ddos-protection protocols dhcpv4 request
clear ddos-protection protocols dhcpv4 request states
clear-ddos-dhcpv4-request-states
clear ddos-protection protocols dhcpv4 request statistics
clear-ddos-dhcpv4-request-statistics
clear ddos-protection protocols dhcpv4 states
clear-ddos-dhcpv4-states
clear ddos-protection protocols dhcpv4 statistics
clear-ddos-dhcpv4-statistics
clear ddos-protection protocols dhcpv4 unclassified
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 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 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-dhcpv6-leaseq-da-states
clear ddos-protection protocols dhcpv6 leasequery-data statistics
clear-ddos-dhcpv6-leaseq-da-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 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 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 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 states
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 states
clear-ddos-dtcp-aggregate-states
clear ddos-protection protocols dtcp aggregate statistics
clear-ddos-dtcp-aggregate-statistics
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 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 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 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 states
clear-ddos-esmc-aggregate-states
clear ddos-protection protocols esmc aggregate statistics
clear-ddos-esmc-aggregate-statistics
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 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 states
clear-ddos-fw-host-aggregate-states
clear ddos-protection protocols firewall-host aggregate statistics
clear-ddos-fw-host-aggregate-statistics
clear ddos-protection protocols firewall-host states
clear-ddos-fw-host-states
clear ddos-protection protocols firewall-host statistics
clear-ddos-fw-host-statistics
clear-ddos-fw-reject-aggregate-statistics
clear-ddos-fw-reject-states
clear ddos-protection protocols ftp
clear ddos-protection protocols ftp aggregate
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 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 states
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 states
<clear-ddos-icmpv6-aggregate-states>
clear ddos-protection protocols icmpv6 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 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-igmpv4v6-aggregate-statistics
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 states
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 igmpv6 statistics
clear-ddos-igmpv6-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-ip-frag-aggregate-statistics
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 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-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 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 states
clear-ddos-ip-opt-unclass-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 states
clear-ddos-isis-aggregate-states
clear ddos-protection protocols isis aggregate statistics
clear-ddos-isis-aggregate-statistics
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 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 l2tp
clear ddos-protection protocols l2tp aggregate
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 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 states
clear-ddos-ldp-aggregate-states
clear ddos-protection protocols ldp aggregate statistics
clear-ddos-ldp-aggregate-statistics
clear ddos-protection protocols ldp states
clear-ddos-ldp-states
```

```
clear ddos-protection protocols ldp statistics
clear-ddos-ldp-statistics
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate states
clear-ddos-ldpv6-aggregate-states
clear ddos-protection protocols ldpv6 aggregate statistics
clear-ddos-ldpv6-aggregate-statistics
clear ddos-protection protocols ldpv6 states
clear-ddos-ldpv6-states
clear ddos-protection protocols ldpv6 statistics
clear-ddos-ldpv6-statistics
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate states
clear-ddos-lddp-aggregate-states
clear ddos-protection protocols lldp aggregate statistics
clear-ddos-lddp-aggregate-statistics
clear ddos-protection protocols lldp states
clear-ddos-lddp-states
clear ddos-protection protocols lldp statistics
clear-ddos-lddp-statistics
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate states
clear-ddos-lmp-aggregate-states
clear ddos-protection protocols lmp aggregate statistics
clear-ddos-lmp-aggregate-statistics
clear ddos-protection protocols lmp states
clear-ddos-lmp-states
clear ddos-protection protocols lmp statistics
clear-ddos-lmp-statistics
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate states
clear-ddos-lmpv6-aggregate-states
clear ddos-protection protocols lmpv6 aggregate statistics
clear-ddos-lmpv6-aggregate-statistics
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 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-mac-host-statistics
clear ddos-protection protocols mlp
clear ddos-protection protocols mlp aggregate
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 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-msdp-aggregate-statistics
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 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-mvrp-aggregate-statistics
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-ndpv6-statistics>clear ddos-protection protocols ntp
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-ntp-aggregate-statistics
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 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-ospf-states
clear ddos-protection protocols ospf statistics
clear-ddos-ospf-statistics
clear ddos-protection protocols ospfv3v6
clear ddos-protection protocols ospfv3v6 aggregate
clear ddos-protection protocols ospfv3v6 aggregate states
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 ospfv3v6 statistics
clear-ddos-ospfv3v6-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-pfe-alive-aggregate-statistics
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-pim-aggregate-statistics
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 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-pmvrp-aggregate-statistics
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 mplscp
clear ddos-protection protocols ppp mplscp states
clear-ddos-ppp-mplscp-states
clear ddos-protection protocols ppp mplscp statistics
clear-ddos-ppp-mplscp-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-ntp-aggregate-states
clear ddos-protection protocols ptp aggregate statistics
clear-ddos-ntp-aggregate-statistics
clear ddos-protection protocols ptp states
clear-ddos-ntp-states
clear ddos-protection protocols ptp statistics
clear-ddos-ntp-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-radius-auth-states
clear ddos-protection protocols radius authorization statistics
clear-ddos-radius-auth-statistics
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 states
<clear-ddos-sample-pfe-states>
clear ddos-protection protocols sample pfe statistics
<clear-ddos-sample-pfe-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 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-sample-tap-states>
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-services-aggregate-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-snmp-aggregate-statistics
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-sshv6-aggregate-statistics
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 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 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 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 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 states
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 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-vrrp-aggregate-statistics
```



```
clear ddos-protection protocols vrrp states
clear-ddos-vrrp-states
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-vrrpv6-statistics
clear dhcp
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 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 relay
clear dhcpv6 relay binding
clear dhcpv6 relay binding interface
clear dhcpv6 relay statistics
<clear-dhcpv6-relay-statistics-information>
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 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 dot1x
clear dot1x interface
<clear-dot1x-interface-session>

clear dot1x mac-address
<clear-dot1x-mac-session>

clear error
clear error bpd
clear error bpd interface
<clear-bpd-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 fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-counters>
clear firewall log
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 statistics
<clear-igmp-snooping-statistics>
clear igmp snooping statistics bridge-domain
<clear-igmp-snooping-bridge-domain-statistics>
clear igmp statistics
<clear-igmp-statistics>
clear ike
clear ike security-associations
<clear-ike-security-associations>
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 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 mac-move-buffer
<clear-l2-learning-mac-move-buffer>
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 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 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 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 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-ospf-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 pfe
clear pfe statistics
clear pfe statistics fabric
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 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 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 software
clear services inline software statistics
<clear-inline-software-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 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 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 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 twamp-information
clear twamp-server-information
clear twamp-server-connection-information
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 interface
clear spanning-tree statistics routing-instance
<clear-stp-routing-instance-statistics>
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 login
clear system login logout
<clear-system-login-logout>

```

```

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 snmp
<request-snmp-utility-mib-clear>
<request-snmp-utility-mib-set>
clear vrrp
clear vrrp interface
request services ipsec-vpn ipsec
request services ipsec-vpn ipsec switch
request services ipsec-vpn ipsec switch tunnel

```

**Configuration Hierarchy Levels** No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## control

Can perform all control-level operations; can modify any configuration.

### Commands

```
test configuration
```

### Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

### Related Documentation

- [Access Privilege User Permission Flags Overview on page 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## field

Can view field debug commands.

### 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## firewall

Can view the firewall filter configuration in configuration mode.

<b>Commands</b>	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>
<b>Configuration Hierarchy Levels</b>	[edit dynamic-profiles firewall] [edit firewall] [edit logical-systems firewall]
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> <li>• <a href="#">firewall-control on page 743</a></li> </ul>

## firewall-control

Can view and configure firewall filter information at the [edit dynamic-profiles firewall], [edit firewall], and [edit logical-systems firewall] hierarchy levels.

<b>Commands</b>	show firewall <get-firewall-information>
	show firewall counter <get-firewall-counter-information>

	<code>show firewall filter</code> <code>&lt;get-firewall-filter-information&gt;</code>
	<code>show firewall filter version</code> <code>&lt;get-filter-version&gt;</code>
	<code>show firewall log</code> <code>&lt;get-firewall-log-information&gt;</code>
	<code>show firewall prefix-action-stats</code> <code>&lt;get-firewall-prefix-action-information&gt;</code>
	<code>show policer</code>
<b>Configuration Hierarchy Levels</b>	<code>[edit dynamic-profiles firewall]</code> <code>[edit firewall]</code> <code>[edit logical-systems firewall]</code>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li><li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li><li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li><li>• <a href="#">firewall on page 743</a></li></ul>

## floppy

	Can read from and write to the removable media.
<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	No associated CLI configuration hierarchy levels and statements.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li><li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li><li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li></ul>

## flow-tap

Can view the flow-tap configuration in configuration mode.

<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	<a href="#">[edit services flow-tap]</a> <a href="#">[edit services radius-flow-tap]</a> <a href="#">[edit system services flow-tap-dtcp]</a>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> <li>• <a href="#">flow-tap-control on page 745</a></li> </ul>

## 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.

<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	<a href="#">[edit services flow-tap]</a> <a href="#">[edit services radius-flow-tap]</a> <a href="#">[edit system services flow-tap-dtcp]</a>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> <li>• <a href="#">flow-tap on page 744</a></li> </ul>

## flow-tap-operation

Can make flow-tap requests to the router.

<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	No associated CLI configuration hierarchy levels and statements.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> </ul>

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)



- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [interface-control on page 747](#)

## 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [interface on page 746](#)

## 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

clear system reboot

<clear-reboot>

clear-system-services-reverse-information

file archive

<file-archive>

monitor traffic

request chassis beacon

<request-chassis-beacon>

request chassis ccg

<request-chassis-ccg>

request chassis cb

request chassis cfeb

request chassis cfeb master

request chassis cip

request chassis fabric

request chassis fabric device

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 mcs

request chassis mic

request chassis pcg

request chassis pic

request chassis redundancy

request chassis redundancy feb

<request-redundancy-feb>

request chassis routing-engine

request chassis routing-engine hard-disk-test

request chassis routing-engine master

request chassis scg

request chassis sfm

request chassis sfm master

request chassis sib

request chassis sib f13

request chassis sib f2s

request chassis spmb

request chassis ssb

request chassis ssb master

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
request chassis tfcb
request chassis vcpu
request chassis vnpu
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 key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate enroll
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 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 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 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 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 system reboot  
    <request-reboot>

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 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 zeroize
request vpls-switchover
set date
set date ntpshow services fips
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]

```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## 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 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 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 mrinfo
ssh
telnet
traceroute
 <traceroute>

traceroute clns
traceroute ethernet
 <request-traceroute-ethernet>

traceroute monitor
traceroute mpls
traceroute mpls ldp
<traceroute-mpls-ldp>
traceroute mpls rsvp
<traceroute-mpls-rsvp>

```

**Configuration Hierarchy Levels** No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## pgcp-session-mirroring

Can view session mirroring configuration by using the **pgcp** command.

<b>Commands</b>	show services pgcp gates gate-way display session-mirroring
<b>Configuration Hierarchy Levels</b>	[edit services pgcp gateway session-mirroring] [edit services pgcp session-mirroring]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [pgcp-session-mirroring-control on page 756](#)

## pgcp-session-mirroring-control

Can modify PGCP session mirroring configuration

- 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [pgcp-session-mirroring on page 755](#)

## 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**
- `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>

```

**Configuration Hierarchy Levels** No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## rollback

Can roll back to previous configurations.

**Commands** rollback

**Configuration Hierarchy Levels** [edit]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)

## routing

Can view general routing, routing protocol, and routing policy configuration information.

**Commands** No associated CLI commands.

**Configuration Hierarchy Levels**

```

[edit bridge-domains]
[edit bridge-domains domain multicast-snooping-options]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols router-advertisement traceoptions]

```

```
[edit dynamic-profiles routing-instances]
[edit dynamic-profiles routing-instances instance bridge-domains]
[edit dynamic-profiles routing-instances instance bridge-domains domain
multicast-snooping-options]
[edit dynamic-profiles routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance pbb-options]
[edit dynamic-profiles routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit dynamic-profiles routing-instances instance switch-options]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit jnx-example]
[edit fabric protocols]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[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 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 isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host 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 ospf traceoptions]
[edit logical-systems protocols pim 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]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit logical-systems routing-instances instance switch-options]
```

```
[edit logical-systems routing-options]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
[edit multicast-snooping-options]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections][edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvrp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance multicast-snooping-options]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[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 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]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-options]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit switch-options]

```

#### Related Documentation

- [Access Privilege User Permission Flags Overview on page 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [routing-control on page 761](#)

## 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.

**Commands** No associated CLI commands.

#### Configuration Hierarchy Levels

```

[edit bridge-domains]
[edit bridge-domains domain multicast-snooping-options]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles routing-instances]
[edit dynamic-profiles routing-instances instance bridge-domains]
[edit dynamic-profiles routing-instances instance bridge-domains domain

```

```
multicast-snooping-options]
[edit dynamic-profiles routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance pbb-options]
[edit dynamic-profiles routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit dynamic-profiles routing-instances instance switch-options]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit jnx-example]
[edit fabric protocols]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[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 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 isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host 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 ospf traceoptions]
[edit logical-systems protocols pim 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]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit logical-systems routing-instances instance switch-options]
[edit logical-systems routing-options]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
```

```
[edit multicast-snooping-options]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections][edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvrp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance multicast-snooping-options]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[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 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]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-options]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit switch-options]
```

#### Related Documentation

- [Access Privilege User Permission Flags Overview on page 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [routing on page 757](#)

## 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 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 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [secret-control on page 766](#)

## 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]
[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 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [secret on page 765](#)

## 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [security-control on page 771](#)

## 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
```

	<pre> &lt;get-idp-detail-status-information&gt; show security keychain &lt;get-hakr-keychain-information&gt; show security log &lt;get-security-log-information&gt;  show security pki show security pki ca-certificate &lt;get-pki-ca-certificate&gt; show security pki certificate-request &lt;get-pki-certificate-request&gt; show security pki crl &lt;get-pki-crl&gt; show security pki local-certificate &lt;get-pki-local-certificate&gt; </pre>
<b>Configuration Hierarchy Levels</b>	<pre> [edit security] [edit security alarms] [edit security log] </pre>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> <li>• <a href="#">security on page 767</a></li> </ul>

## shell

	Can start a local shell on the router.
<b>Commands</b>	<pre> start shell start shell user </pre>
<b>Configuration Hierarchy Levels</b>	No associated CLI configuration hierarchy levels and statements.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> </ul>

## snmp

Can view Simple Network Management Protocol (SNMP) configuration.

<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	[edit snmp]
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> </ul>

## system

Can view system-level configuration information.

<b>Commands</b>	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
<b>Configuration Hierarchy Levels</b>	[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 logical-systems system syslog]  [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 no-debugger-on-alt-break]
[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 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 vlans]
```

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [system-control on page 777](#)

## system-control

Can view system-level configuration information and configure it at the **[edit system]** hierarchy level.

<b>Configuration</b>	[edit applications]
<b>Hierarchy Levels</b>	[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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [system on page 775](#)

## 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 bridge-domains domain multicast-snooping-options traceoptions]
[edit bridge-domains domain protocols igmp-snooping]
[edit bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit bridge-domains domain protocols igmp-snooping traceoptions]
[edit bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit bridge-domains 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]
[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 bridge-domains domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay
traceoptions]
[edit logical-systems bridge-domains domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems bridge-domains 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 bridge-domains domain
multicast-snooping-options traceoptions]
```

```
[edit logical-systems routing-instances instance bridge-domains 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 bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance bridge-domains 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 703](#)
  - [Understanding Junos OS Access Privilege Levels on page 669](#)
  - [Configuring Access Privilege Levels on page 694](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
  - [trace-control on page 783](#)

## trace-control

Can modify trace file settings and configure trace file properties

### Configuration Hierarchy Levels

```
[edit bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
[edit bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit bridge-domains 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]
[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 bridge-domains domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems bridge-domains domain forwarding-options dhcp-relay
traceoptions]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]  
[edit logical-systems routing-instances instance bridge-domains domain forwarding-options dhcp-relay traceoptions]  
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]  
[edit logical-systems routing-instances instance bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance bridge-domains domain forwarding-options dhcp-relay
traceoptions]
[edit routing-instances instance bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance bridge-domains 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 703](#)
- [Understanding Junos OS Access Privilege Levels on page 669](#)
- [Configuring Access Privilege Levels on page 694](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 695](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697](#)
- [trace on page 778](#)

**view**

Can view current system-wide, routing table, and protocol-specific values and statistics.

**Commands**

```
clear ipv6 router-advertisement
<clear-ipv6-router-advertisement-information>

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 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 subscriber
 <get-ancp-subscriber-information>

show ancp subscriber identifier
 <get-ancp-subscriber-identifier-information>
show ancp subscriber neighbor
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 bfd
show bfd session
 <get-bfd-session-information>

show bfd session address
 <get-bfd-session-address>
show bfd session discriminator
 <get-bfd-session-discriminator>
show bfd session prefix
 <get-bfd-session-prefix>
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>
 <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 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 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 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 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 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 fabric
show chassis fabric device
 <get-chassis-fabric-information-device>
show chassis fabric connectivity
 <get-chassis-fabric-connectivity-information>
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 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 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 temperature-thresholds
 <get-temperature-threshold-information>
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 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 rewrite-rule
 <get-cos-rewrite-information>

show class-of-service routing-instance
 <get-cos-routing-instance-map-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
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 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 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 dhcpv6
get-ddos-dhcpv6-information
show ddos-protection protocols dhcpv6 advertise
get-ddos-dhcpv6-advertise
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-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 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 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-ftp6-information
show ddos-protection protocols ftpv6 aggregate
```



```
get-ddos-ftp6-aggregate
show ddos-protection protocols ftpv6 parameters
 get-ddos-ftp6-parameters
show ddos-protection protocols ftpv6 statistics
 get-ddos-ftp6-statistics
show ddos-protection protocols ftpv6 violations
 get-ddos-ftp6-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 parameters
 get-ddos-gre-parameters
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 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 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 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 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 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 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 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 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 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 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 pimv6
<get-ddos-pimv6-information>
show ddos-protection protocols pimv6 aggregate
<get-ddos-pimv6-aggregate>
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 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 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 lcp
```

```
get-ddos-ppp-lcp
show ddos-protection protocols ppp mplsdp
get-ddos-ppp-mplsdp
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 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 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 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 rip
get-ddos-rip-information
show ddos-protection protocols rip aggregate
get-ddos-rip-aggregate
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 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 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 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 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 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 violations
 <get-ddos-sample-violations>
show ddos-protection protocols services
 get-ddos-services-information
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 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 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 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 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 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 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 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 statistics
<get-ddos-uncls-statistics>
show ddos-protection protocols unclassified violations
<get-ddos-uncls-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 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 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 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 dhcp
```

```
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 statistics
 <get-dhcp-relay-statistics-information>

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 statistics
 <get-dhcp-server-statistics-information>
show dhcp statistics
 <get-dhcp-service-statistics-information>
show dhcpv6
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 statistics
 <get-dhcpv6-relay-statistics-information>
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 statistics
 <get-dhcpv6-server-statistics-information>
show dhcpv6 statistics
 <get-dhcpv6-service-statistics-information>
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-tunnels
show dynamic-tunnels database
 <get-dynamic-tunnels-database>
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>

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-mspinfo-virtual-memory>
 <get-mac-ip-binding-information>
 <get-mc-ccpc-src-mod-filters>
 <get-core-key-list>
 <get-mc-edge-map-to-key-binding>
 <get-key-vg-binding>
 <get-mc-edge-key-to-map-binding>
 <get-mc-edge-vg-portmap>
 <get-mc-nsf>
 <get-mc-root-map-to-key-binding>
 <get-mc-root-key-to-map-binding>
 <get-mc-root-vg-pfemap>
 <get-mc-vccpdf-adjacency-database>
 <get-fabric-summary-information>
get-fabric-statistics
get-fabric-summary-information
 <get-vlan-domain-map-information>
show forwarding-options
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 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 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 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 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 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 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 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 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 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 path
 <get-ldp-path-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 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 interface
 <get-mpls-interface-information>

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-route>
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 ntp
show ntp associations
show ntp status
show oam
show oam ethernet
show oam ethernet connectivity-fault-management
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 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 pfe
show pfe cfeb
show pfe feb
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 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 fabric
show pfe statistics ip
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 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 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-ptp-clock>
show ptp global-information
 get-ptp-global-information>
show ptp hybrid
show ptp hybrid config
 <get-ptp-hybrid-mapping>
show ptp hybrid status
 <get-ptp-hybrid-status>
show ptp last-tod-update
 <get-last-tod-update>
show ptp lock-status
 get-ptp-lock-status>
show ptp master
 <get-ptp-master>
show ptp port
 <get-ptp-port>
show ptp quality-level-mapping
 <get-ptp-quality-level-mapping>
show ptp slave
 <get-ptp-slave>
show ptp statistics
 <get-ptp-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 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 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 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 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 nat
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 ipsec-vpn
show services ipsec-vpn ike
show services ipsec-vpn ike security-associations
 <get-ike-services-security-associations-information>

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 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 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
show services nat mappings endpoint-independent
 <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 summary
 <get-service-nat-mapping-summary>
show services nat pool
 <get-service-nat-pool-information>

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 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 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 softwire
 <get-service-softwire-table-information>

show services softwire flows
 <get-service-fwnat-flow-table-information>

show services softwire statistics
 <get-service-softwire-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 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 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 interface
show spanning-tree statistics routing-instance
 <get-stp-routing-instance-statistics>
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 boot-messages
show system buffers
show system certificate
show system commit
 <get-commit-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 license
 <get-license-summary-information>

show system license installed
 <get-license-information>

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 extensive
show system processes health
```

```
<get-process-health-information>

show system processes providers
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>

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 vpls
show system storage
 <get-system-storage>
show system storage partitions
```

```
<get-system-storage-partitions>
show system subscriber-management
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 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 version
 <get-software-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 fdl-line-loop
test interface fdl-line-loop ansi
test interface fdl-line-loop ansi initiate
test interface fdl-line-loop ansi terminate
test interface fdl-line-loop bellcore
test interface fdl-line-loop bellcore initiate
test interface fdl-line-loop bellcore terminate
test interface fdl-payload-loop
test interface fdl-payload-loop ansi
test interface fdl-payload-loop ansi initiate
test interface fdl-payload-loop ansi terminate
test interface fdl-payload-loop bellcore
test interface fdl-payload-loop bellcore initiate
test interface fdl-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
<
```



<b>Configuration Hierarchy Levels</b>	<p>[edit dynamic-profiles routing-instances instance services mobile-ip home-agent enable-service]</p> <p>[edit logical-systems routing-instances instance services mobile-ip home-agent enable-service]</p> <p>[edit logical-systems services mobile-ip home-agent enable-service]</p> <p>[edit routing-instances instance services mobile-ip home-agent enable-service]</p> <p>[edit services mobile-ip home-agent enable-service]</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> </ul>

## view-configuration

Can view all of the configuration (not including secrets).

<b>Commands</b>	No associated CLI commands.
<b>Configuration Hierarchy Levels</b>	No associated CLI configuration hierarchy levels and statements.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Access Privilege User Permission Flags Overview on page 703</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 669</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 694</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 695</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 697</a></li> </ul>

## Configuring Authentication Methods

- [Configuring RADIUS Server Authentication on page 851](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 855](#)
- [Configuring TACACS+ Authentication on page 857](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 859](#)
- [Example: Configuring Authentication Order on page 862](#)

## 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 9ABC123 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 9ABC123
```

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 855](#)
- [Overview on page 855](#)
- [Configuration on page 855](#)
- [Verification on page 857](#)

### 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, and then 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* 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 862](#).
- Configure a user. See [“Example: Configuring New Users” on page 674](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 677](#).

### 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 673](#)
- [Understanding User Accounts on page 667](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 859](#)
- [Understanding Login Classes on page 663](#)

## Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the device. Tasks to configure TACACS+ configuration are:

- [Configuring TACACS+ Server Details on page 857](#)
- [Specifying a Source Address for the Junos OS to Access External TACACS+ Servers on page 858](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 858](#)
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 859](#)

### Configuring TACACS+ Server Details

---

To use TACACS+ authentication on the device, 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 device 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 device must match that used by the server.

Optionally, you can specify the length of time that the local device waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the device 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 device 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 device 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+ Server Details*.



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 "9ABC123"; ## SECRET-DATA
 10.3.3.3 secret "9ABC123"; ## 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

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication](#)

### Example: Configuring a TACACS+ Server for System Authentication

This example shows how to configure a TACACS+ server for system authentication.

- [Requirements on page 860](#)
- [Overview on page 860](#)
- [Configuration on page 860](#)
- [Verification on page 861](#)

## 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, and then 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* 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 862](#).
- Configure a user. See [“Example: Configuring New Users” on page 674](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 677](#).

---

## Verification

Confirm that the configuration is working properly.

### *Verifying the TACACS+ Server System Authentication Configuration*

<b>Purpose</b>	Verify that the TACACS+ server has been configured for system authentication.
<b>Action</b>	From operational mode, enter the <b>show system tacplus-server</b> command.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding User Authentication Methods on page 673</a></li><li>• <a href="#">Understanding User Accounts on page 667</a></li><li>• <a href="#">Example: Configuring a RADIUS Server for System Authentication on page 855</a></li><li>• <a href="#">Understanding Login Classes on page 663</a></li></ul>

## Example: Configuring Authentication Order

This example shows how to configure authentication order.

- [Requirements on page 862](#)
- [Overview on page 862](#)
- [Configuration on page 862](#)
- [Verification on page 864](#)

### 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

---

<b>CLI Quick Configuration</b>	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 <b>[edit]</b> hierarchy level, and then enter <b>commit</b> from configuration mode.
--------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

<b>GUI Step-by-Step Procedure</b>	<p>To configure authentication order:</p> <ol style="list-style-type: none"><li>1. In the J-Web user interface, select <b>Configure&gt;System Properties&gt;User Management</b>.</li><li>2. Click <b>Edit</b>. The Edit User Management dialog box appears.</li></ol>
-----------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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* 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 855](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 859](#).
- Configure a user. See [“Example: Configuring New Users” on page 674](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 677](#).

---

### 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 673](#)
- [Understanding User Accounts on page 667](#)
- [Understanding Login Classes on page 663](#)

## CHAPTER 28

# Configuring Remote Access to an SRX Series Appliances

- [Configuring Secure Web Access on page 865](#)
- [Setting up USB Modems for Remote Management on page 872](#)
- [Configuring Telnet and SSH Access to an SRX Series Appliance on page 887](#)

## Configuring Secure Web Access

---

- [Secure Web Access Overview on page 865](#)
- [Generating an SSL Certificate Using the openssl Command on page 866](#)
- [Generating a Self-Signed SSL Certificate on page 866](#)
- [Manually Generating Self-Signed SSL Certificates on page 867](#)
- [Configuring Device Addresses on page 868](#)
- [Enabling Access Services on page 868](#)
- [Example: Configuring Secure Web Access on page 869](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 871](#)

## 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 866](#)
- [Generating a Self-Signed SSL Certificate on page 866](#)
- [Configuring Device Addresses on page 868](#)
- [Example: Configuring Secure Web Access on page 869](#)

## 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 865](#)

## 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 866](#)

## 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 866](#)

## 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 868](#)

## 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 868](#)

### Example: Configuring Secure Web Access

This example shows how to configure secure Web access on your device.

- [Requirements on page 869](#)
- [Overview on page 869](#)
- [Configuration on page 870](#)
- [Verification on page 871](#)

#### 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, and then 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* 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/Ts66DZoXI4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
 ... KYiFf4CbBBbjlMQJOHFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
 eIQBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
 CERTIFICATE----- \nMIIDjDCCA vWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
 FADCBkTElMAKGAIUEBhMCdXMx\nCzAJBgNVBAGTA mNhMRIwEAYDVQQHEWlzdW5ue
 HB1YnMxDTALBgNVBAMTBGpucHl xJDAiBgkqhkiG\n9w0BCQEFWF5iaGFyZ2F2YUB
 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 871](#)
- [Verifying a Secure Access Configuration on page 871](#)

#### *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 865](#)
  - [Generating an SSL Certificate Using the openssl Command on page 866](#)
  - [Generating a Self-Signed SSL Certificate on page 866](#)
  - [Configuring Device Addresses on page 868](#)

## 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 866](#)

---

## Setting up USB Modems for Remote Management

---

- [USB Modem Interface Overview on page 872](#)
- [USB Modem Configuration Overview on page 875](#)
- [Example: Configuring a USB Modem Interface on page 877](#)
- [Example: Configuring a Dialer Interface on page 879](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 883](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 885](#)
- [Connecting to the Device Remotely on page 886](#)
- [Modifying USB Modem Initialization Commands on page 886](#)
- [Resetting USB Modems on page 887](#)

### 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 **umd0**. 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 91 on page 874](#) describes the commands. For more information about these commands, see the documentation for your modem.

**Table 91: Default Modem Initialization Commands**

Modem Command	Description
<b>AT</b>	Attention. Informs the modem that a command follows.
<b>S7=45</b>	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
<b>S0=0</b>	Disables the auto answer feature, whereby the modem automatically answers calls.
<b>V1</b>	Displays result codes as words.
<b>&amp;C1</b>	Disables reset of the modem when it loses the carrier signal.
<b>E0</b>	Disables the display on the local terminal of commands issued to the modem from the local terminal.
<b>Q0</b>	Enables the display of result codes.
<b>&amp;Q8</b>	Enables Microcom Networking Protocol (MNP) error control mode.
<b>%C0</b>	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.



**NOTE:** On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), keepalives do not get exchanged, and the interface goes down.

#### Related Documentation

- [USB Modem Configuration Overview on page 875](#)
- [Example: Configuring a USB Modem Interface on page 877](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 883](#)

## 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 from US Robotics (<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 92 on page 876](#) for a summarized description of the procedure.

**Table 92: 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 <a href="#">“Example: Configuring a USB Modem Interface” on page 877</a> .
	Configure the dialer interface <b>dl0</b> on the branch office router using one of the following backup methods: <ul style="list-style-type: none"> <li>Configure the dialer interface <b>dl0</b> as the backup interface on the branch office router's primary T1 interface <b>t1-1/0/0</b>.</li> <li>Configure a dialer filter on the branch office router's dialer interface.</li> <li>Configure a dialer watch on the branch office router's dialer interface.</li> </ul>	Configure the dialer interface using one of the following backup methods: <ul style="list-style-type: none"> <li>To configure <b>dl0</b> as a backup for <b>t1-1/0/0</b> see <a href="#">Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</a>.</li> <li>To configure a dialer filter on <b>dl0</b>, see <a href="#">Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</a>.</li> <li>To configure a dialer watch on <b>dl0</b>, see <a href="#">Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup</a>.</li> </ul>
Head Office	Configure dial-in on the dialer interface <b>dl0</b> on the head office router.	To configure dial-in on the head office router, see <a href="#">“Example: Configuring a Dialer Interface for USB Modem Dial-In” on page 883</a> .

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 93 on page 877](#) for a list of available incoming map options.

Table 93: Incoming Map Options

Option	Description
<b>accept-all</b>	<p>Dialer interface accepts all incoming calls.</p> <p>You can configure the <b>accept-all</b> option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the <b>accept-all</b> option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.</p>
<b>caller</b>	<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 872](#)
- [Example: Configuring a USB Modem Interface on page 877](#)

## Example: Configuring a USB Modem Interface

This example shows how to configure a USB modem interface for dial backup.

- [Requirements on page 877](#)
- [Overview on page 877](#)
- [Configuration on page 878](#)
- [Verification on page 878](#)

### 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 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, 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* 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 : ATS0=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 875](#)
  - [USB Modem Interface Overview on page 872](#)
  - [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 883](#)

**Example: Configuring a Dialer Interface**

This example shows how to configure a logical dialer interface for the device.

- [Requirements on page 880](#)
- [Overview on page 880](#)

- [Configuration on page 880](#)
- [Verification on page 882](#)

## 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, and then 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* 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, Runt: 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 872](#)
  - [USB Modem Configuration Overview on page 875](#)
  - [Example: Configuring a USB Modem Interface on page 877](#)
  - [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 883](#)

## 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 883](#)
- [Overview on page 883](#)
- [Configuration on page 884](#)
- [Verification on page 884](#)

### 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, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
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 875](#)
- [Example: Configuring a USB Modem Interface on page 877](#)

## 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 872](#)
- [USB Modem Configuration Overview on page 875](#)
- [Connecting to the Device Remotely on page 886](#)

## 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 872](#)
- [USB Modem Configuration Overview on page 875](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 885](#)

## 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 872](#)
- [USB Modem Configuration Overview on page 875](#)
- [Resetting USB Modems on page 887](#)

## 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 872](#)
- [USB Modem Configuration Overview on page 875](#)
- [Modifying USB Modem Initialization Commands on page 886](#)

## Configuring Telnet and SSH Access to an SRX Series Appliance

---

- [Securing the Console Port Configuration Overview on page 888](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 889](#)
- [Configuring Reverse Telnet and Reverse SSH on page 890](#)
- [Example: Controlling Management Access on SRX Series Devices on page 890](#)
- [Example: Configuring a Filter to Block Telnet and SSH Access on page 893](#)
- [The telnet Command on page 898](#)
- [The ssh Command on page 899](#)
- [Configuring Outbound SSH Service on page 900](#)

## 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 into 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 898](#)
- [The ssh Command on page 899](#)

- [Configuring Password Retry Limits for Telnet and SSH Access on page 889](#)
- [Configuring Reverse Telnet and Reverse SSH on page 890](#)

## 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 898](#)
- [The ssh Command on page 899](#)
- [Configuring Reverse Telnet and Reverse SSH on page 890](#)

## 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 898](#)
- [The ssh Command on page 899](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 889](#)

## Example: Controlling Management Access on SRX Series Devices

This example shows how to control management access on SRX Series devices.

- [Requirements on page 891](#)
- [Overview on page 891](#)



- [Configuration on page 891](#)
- [Verification on page 893](#)

## 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 891](#)

### *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, and then 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* 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 888](#)

### Example: Configuring a Filter to Block Telnet and SSH Access

- [Requirements on page 894](#)
- [Overview on page 894](#)
- [Configuration on page 894](#)
- [Verification on page 896](#)

## 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*.

To configure this example, perform the following tasks:

- [Configure the Stateless Firewall Filter on page 894](#)
- [Apply the Firewall Filter to the Loopback Interface on page 895](#)
- [Confirm and Commit Your Candidate Configuration on page 895](#)

### CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
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 default-term 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 896](#)
- [Verifying Logged and Rejected Packets on page 897](#)

### **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 '^J'.

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 890](#)

## 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 SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum number of concurrent Telnet sessions is as follows:

SRX100	SRX210	SRX220	SRX240	SRX650
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 94 on page 899 describes the **telnet** command options.

**Table 94: CLI telnet Command Options**

Option	Description
<b>8bit</b>	Use an 8-bit data path.
<b>bypass-routing</b>	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.
<b>host</b>	Open a Telnet session to the specified hostname or IP address.
<b>inet</b>	Force the Telnet session to an IPv4 destination.
<b>interface <i>source-interface</i></b>	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
<b>no-resolve</b>	Suppress the display of symbolic names.
<b>port <i>port</i></b>	Specify the port number or service name on the host.
<b>routing-instance <i>routing-instance-name</i></b>	Use the specified routing instance for the Telnet session.
<b>source <i>address</i></b>	Use the specified source address for the Telnet session.

- Related Documentation**
- [The ssh Command on page 899](#)
  - [Configuring Password Retry Limits for Telnet and SSH Access on page 889](#)
  - [Configuring Reverse Telnet and Reverse SSH on page 890](#)

## 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 SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum number of concurrent SSH sessions is as follows:

SRX100	SRX210	SRX220	SRX240	SRX650
3	3	3	5	5

Table 95 on page 900 describes the **ssh** command options.

**Table 95: CLI ssh Command Options**

Option	Description
<b>bypass-routing</b>	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.
<b>host</b>	Open an SSH connection to the specified hostname or IP address.
<b>inet</b>	Force the SSH connection to an IPv4 destination.
<b>interface <i>source-interface</i></b>	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
<b>routing-instance <i>routing-instance-name</i></b>	Use the specified routing instance for the SSH connection.
<b>source address</b>	Use the specified source address for the SSH connection.
<b>v1</b>	Force SSH to use version 1 for the connection.
<b>v2</b>	Force SSH to use version 2 for the connection.

- Related Documentation**
- [The telnet Command on page 898](#)
  - [Configuring Password Retry Limits for Telnet and SSH Access on page 889](#)
  - [Configuring Reverse Telnet and Reverse SSH on page 890](#)

## 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 901](#)
- [Sending the Public SSH Host Key to the Outbound SSH Client on page 901](#)
- [Configuring Keepalive Messages for Outbound SSH Connections on page 902](#)
- [Configuring a New Outbound SSH Connection on page 902](#)
- [Configuring the Outbound SSH Client to Accept NETCONF as an Available Service on page 903](#)
- [Configuring Outbound SSH Clients on page 903](#)

---

### 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

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-host-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 902.

### 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.

---



## CHAPTER 29

# Configuring DNS

- [Configuring DNS Server Caching, DNSSEC, and DNS Proxy on page 905](#)

## Configuring DNS Server Caching, DNSSEC, and DNS Proxy

---

- [DNS Overview on page 905](#)
- [Example: Configuring the TTL Value for DNS Server Caching on page 906](#)
- [DNSSEC Overview on page 907](#)
- [Example: Configuring DNSSEC on page 907](#)
- [Example: Configuring Keys for DNSSEC on page 908](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 908](#)
- [DNS Proxy Overview on page 910](#)
- [Configuring the Device as a DNS Proxy on page 914](#)

## 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 905](#)
- [DNS Server Caching on page 906](#)

## 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 906](#)
- [DNSSEC Overview on page 907](#)

## 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 906](#)
- [Overview on page 906](#)
- [Configuration on page 906](#)
- [Verification on page 907](#)

## 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 905](#)

### 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 905](#)
- [Example: Configuring Keys for DNSSEC on page 908](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 908](#)

### 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 907](#)

### 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 907](#)  
• [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 908](#)

### 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 908](#)
- [Overview on page 908](#)
- [Configuration on page 909](#)

#### 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 907](#)" 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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.25633CJ5K3h
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.25633CJ5K3h"
```

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.25633CJ5K3h; ## 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 907](#)
  - [Example: Configuring Keys for DNSSEC on page 908](#)

## DNS Proxy Overview

A dynamic name service (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 910](#)
- [DNS Proxy with Split DNS on page 910](#)
- [Dynamic Domain Name System Client on page 912](#)

---

### 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

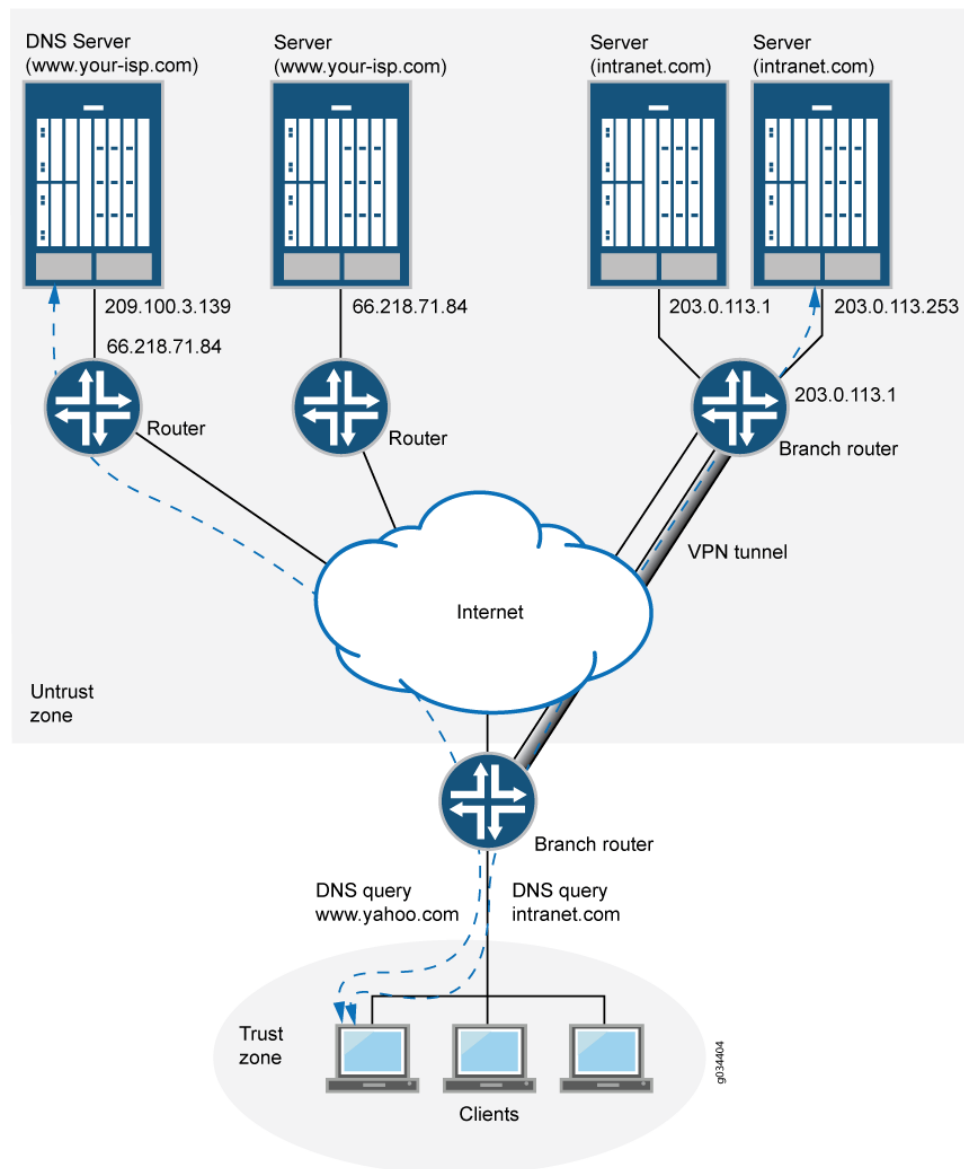
The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name. When you query that domain name, the device sends the DNS queries to 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 55: DNS Proxy with Split DNS



In the corporate network shown in [Figure 55 on page 911](#), 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 (1.1.1.253), 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 56: Dynamic DNS

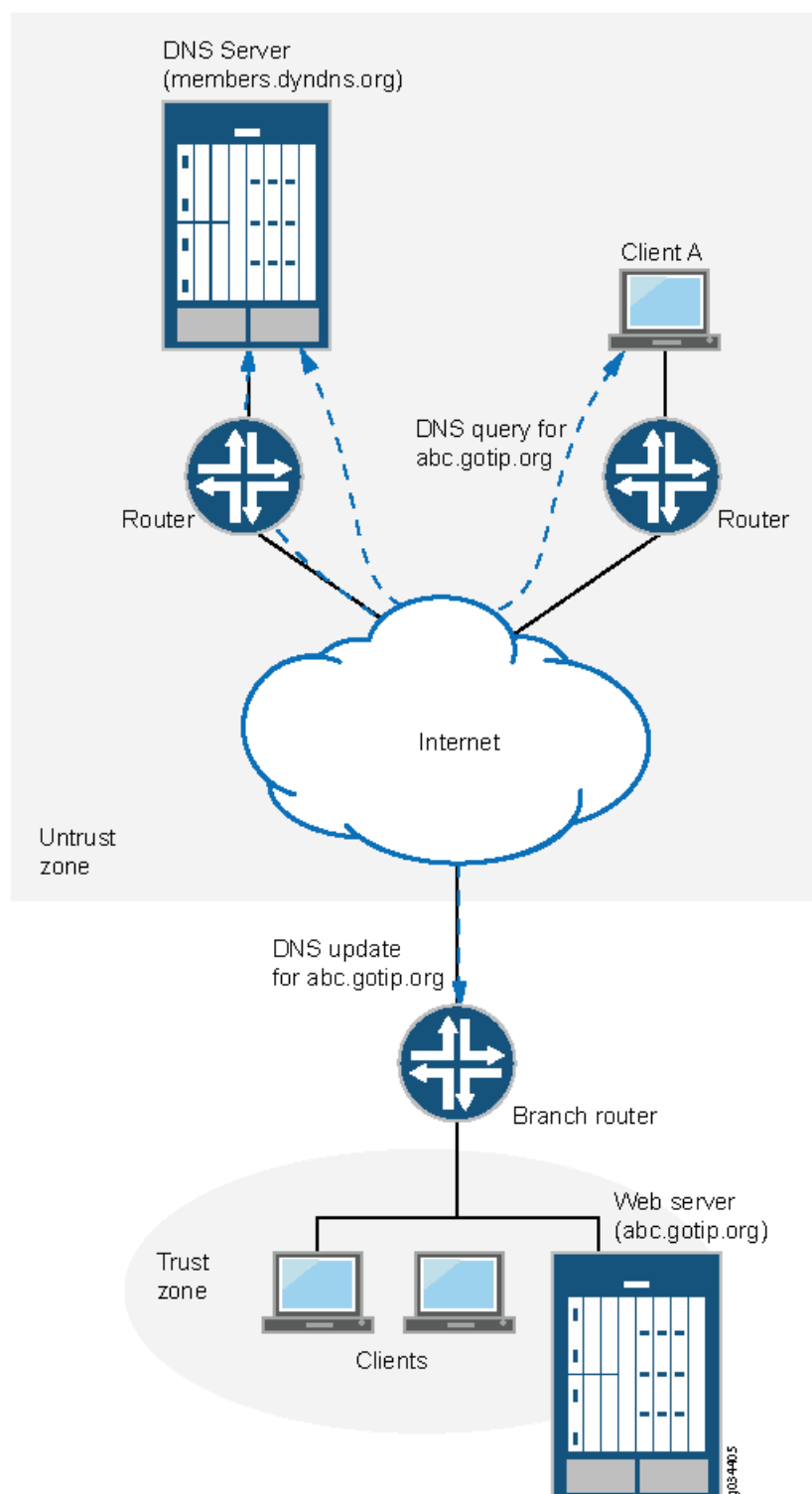


Figure 56 on page 913 illustrates how the DDNS client works. The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the

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 56 on page 913](#) 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 914](#)

## 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.juniper.net`) in addition to using the routable IP address (207.17.137.68 for `www.juniper.net`).

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@hostshow 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@hostshow system services dynamic-dns
```

## Related Documentation

- [Configuring the Device as a DNS Proxy on page 914](#)



# Configuring DHCP Access Service for IP Address Management

- [Understanding DHCP Services on page 917](#)
- [Configuring a DHCP Local Server on page 922](#)
- [Configuring a DHCP Client on page 935](#)
- [Configuring a DHCP Relay Agent on page 942](#)
- [Configuring a DHCPv6 Local Server on page 949](#)
- [Configuring a DHCPv6 Client on page 958](#)
- [Configuring DHCP in Chassis Cluster Mode on page 965](#)

## Understanding DHCP Services

---

- [DHCP Overview on page 917](#)
- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
- [DHCP Settings and Restrictions Overview on page 921](#)

### 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 DHCP client in chassis cluster mode.

### Related Documentation

- [Understanding DHCP Server Operation on page 922](#)
- [Understanding DHCP Client Operation on page 935](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)

## 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 924](#)
- [Understanding DHCP Server Operation on page 922](#)
- [Understanding DHCP Client Operation on page 935](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)
- [DHCP Settings and Restrictions Overview on page 921](#)

## DHCP Settings and Restrictions Overview

This section contains the following topics:

- [Propagation of TCP/IP Settings for DHCP on page 921](#)
- [DHCP Conflict Detection and Resolution on page 922](#)
- [DHCP Interface Restrictions on page 922](#)

### 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 920](#)
- [Understanding DHCP Server Operation on page 922](#)
- [Understanding DHCP Client Operation on page 935](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)

## Configuring a DHCP Local Server

---

- [Understanding DHCP Server Operation on page 922](#)
- [DHCP Server Configuration Overview on page 924](#)
- [Minimum DHCP Local Server Configuration on page 925](#)
- [Configuring Address-Assignment Pools on page 926](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 926](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 927](#)
- [Configuring Static Address Assignments on page 927](#)
- [Enabling TCP/IP Propagation on a DHCP Local Server on page 928](#)
- [Verifying and Managing DHCP Local Server Configuration on page 928](#)
- [Example: Configuring the Device as a DHCP Server on page 929](#)

### 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.



**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.

This section contains the following topics:

- [DHCP Options on page 923](#)
- [Compatibility with Autoinstallation on page 923](#)
- [Chassis Cluster Support on page 923](#)

### 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 920](#)
- [Example: Configuring the Device as a DHCP Server on page 929](#)
- [Understanding DHCP Client Operation on page 935](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)

## 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 96 on page 924](#) provides the settings and values for the sample DHCP server configuration.

**Table 96: Sample DHCP Server Configuration Settings**

Setting	Sample Value
<b>DHCP Subnet Configuration</b>	
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
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
<b>DHCP MAC Address Configuration</b>	
Static binding MAC address	01:03:05:07:09:0B

Table 96: Sample DHCP Server Configuration Settings (*continued*)

Setting	Sample Value
Fixed address	192.168.2.50

**Related Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
- [Understanding DHCP Server Operation on page 922](#)
- [Understanding DHCP Client Operation on page 935](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)
- [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 926](#)

## 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 926](#).
2. (Optional) Configure named ranges (subsets) of addresses.  
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 927](#).
3. (Optional; IPv4 only) Create static address bindings.  
See [“Configuring Static Address Assignments” on page 927](#).
4. (Optional) Configure attributes for DHCP clients.  
See [“Configuring DHCP Client-Specific Attributes for Address-Assignment Pools” on page 936](#).

**Related Documentation** • [Configuring an Address-Assignment Pool Name and Addresses on page 926](#)

### 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 926](#)

## 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_1 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 926](#)

## 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 926](#)

## 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 925](#)

## 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 925](#)

## Example: Configuring the Device as a DHCP Server

This example shows how to configure the device as a DHCP server.

- [Requirements on page 929](#)
- [Overview on page 930](#)
- [Configuration on page 930](#)
- [Verification on page 933](#)

### Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

## Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the default-lease-time to 1,209,600 and the maximum-lease-time to 2,419,200. You then set the domain search suffixes as mycompany.net and mylab.net. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.

Then you specify the DNS server IP address as 192.168.10.2. You set the IP address for the device solicitation address option (option 32) as 192.168.2.33. The IP address excluded from the IP address pool is reserved for this option. Finally, you assign a fixed IP address as 192.168.2.50 with the MAC address of the client, 01:03:05:07:09:0B.

## 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, and then enter **commit** from configuration mode.

```
set system services dhcp pool 192.168.2.0/24 address-range low 192.168.2.2
high 192.168.2.254
set system services dhcp pool 192.168.2.0/24 default-lease-time 1209600
maximum-lease-time 2419200
set system services dhcp pool 192.168.2.0/24 domain-search mycompany.net
set system services dhcp pool 192.168.2.0/24 domain-search mylab.net
set system services dhcp pool 192.168.2.0/24 name-server 192.168.10.2
set system services dhcp pool 192.168.2.0/24 option 32 ip-address 192.168.2.33
set system services dhcp static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50
```

### GUI Step-by-Step Procedure

To configure the device as a DHCP server:

1. In the J-Web interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Next to System, click **Configure**.
3. Next to Services, make sure the check box is selected, and click **Configure**.
4. Next to Dhcp, click **Configure**.
5. Define the IP address pool. Next to Pool, click **Add new entry**.
6. In the Subnet address box, type **192.168.2.0/24**.
7. Next to Address range, select the check box.
8. In the High box, type **192.168.2.254**.
9. In the Low box, type **192.168.2.2**.
10. Click **OK**.
11. Define the default and maximum lease times, in seconds. From the Default lease time list, select **Enter Specific Value**.
12. In the Length box, type **1209600**.



13. From the Maximum lease time list, select **Enter Specific Value**.
14. Next to Maximum lease time, type **2419200**.
15. Define the domain search suffixes to be used by the clients. Next to Domain search, click **Add new entry**.
16. In the Suffix box, type **mycompany.net**.
17. Click **OK**.
18. Next to Domain search, click **Add new entry**.
19. In the Suffix box, type **mylab.net**.
20. Click **OK**.
21. Define a DNS server. Next to Name server, click **Add new entry**.
22. In the Address box, type **192.168.10.2**.
23. Click **OK**.
24. Define DHCP option 32, the device solicitation address option. Next to Option, click **Add new entry**.
25. In the Option identifier code box, type **32**.
26. From the Option type choice list, select **Ip address**.
27. In the Ip address box, type **192.168.2.33**.
28. Click **OK** twice.
29. Assign a static IP address to a MAC address. Next to Static binding, click **Add new entry**.
30. In the Mac address box, type **01:03:05:07:09:0B**.
31. Next to Fixed address, click **Add new entry**.
32. In the Address box, type **192.168.2.50**.
33. Click **OK** until you return to the Configuration page.
34. Click **OK** to check your configuration and save it as a candidate configuration.
35. 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* in the *CLI User Guide*.

To configure the device as a DHCP server:

1. Configure the DHCP server.  

```
[edit]
user@host# edit system services dhcp
```
2. Specify the IP address pool range.  

```
[edit system services dhcp]
```

```
user@host# set pool 192.168.2.0/24 address-range low 192.168.2.2 high 192.168.2.254
```

3. Define the default and maximum lease times, in seconds.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 default-lease-time 1209600
maximum-lease-time 2419200
```

4. Define the domain search suffixes to be used by the clients.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 domain-search mycompany.net
user@host# set pool 192.168.2.0/24 domain-search mylab.net
```

5. Specify the DNS server IP address.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 name-server 192.168.10.2
```

6. Set the device solicitation IP address.

```
[edit system services dhcp]
user@host# set pool 192.168.2.0/24 option 32 ip-address 192.168.2.33
```

7. Assign a fixed IP address with the MAC address of the client.

```
[edit system services dhcp]
user@host# set static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50
```

**Results** From configuration mode, confirm your configuration by entering the **show system services dhcp** 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 services dhcp
pool 192.168.2.0/24 {
 address-range low 192.168.2.2 high 192.168.2.254;
 maximum-lease-time 2419200;
 default-lease-time 1209600;
 name-server {
 192.168.10.2;
 }
 domain-search {
 mycompany.net;
 mylab.net;
 }
 option 32 ip-address 192.168.2.33;
 }
 static-binding 01:03:05:07:09:0B {
 fixed-address {
 192.168.2.50;
 }
 }
}
```

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

## Verification

Confirm that the configuration is working properly.

- [Verifying Global DHCP Information on page 933](#)
- [Verifying the DHCP Binding Database on page 933](#)
- [Verifying DHCP Server Operation on page 934](#)

### Verifying Global DHCP Information

**Purpose** Verify that the global DHCP Information has been configured for the device.

**Action** From operational mode, enter the **show system services dhcp global** command.

```
Global settings:
 BOOTP lease length infinite
 DHCP lease times:
 Default lease time 1 day
 Minimum lease time 1 minute
 Maximum lease time infinite

DHCP options:
 Name: domain-name, Value: mylab.example.net
 Name: name-server, Value: [192.168.5.68, 172.17.28.101, 172.17.28.100]
```

### Verifying the DHCP Binding Database

**Purpose** Verify that the DHCP binding database reflects the DHCP server configuration.

**Action** From operational mode, enter these commands:

- **show system services dhcp binding** command to display all active bindings in the database.
- **show system services dhcp binding *address* detail** command (where *address* is the IP address of the client) to display more information about a client.
- **show system services dhcp conflict command** to show any potential conflicts with the bindings.

These commands produce following sample output:

```
user@host> show system services dhcp binding

IP Address Hardware Address Type Lease expires at
30.1.1.20 00:12:1e:a9:7b:81 dynamic 2007-05-11 11:14:43 PDT

user@host> show system services dhcp binding 3.3.3.2 detail

IP address 3.3.3.2
Hardware address 00:a0:12:00:13:02
Pool 3.3.3.0/24
Interface fe-0/0/0, relayed by 3.3.3.200

Lease information:
Type DHCP
Obtained at 2004-05-02 13:01:42 PDT
```

```
Expires at 2004-05-03 13:01:42 PDT
State active
```

DHCP options:

```
Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
Name: domain-name, Value: mydomain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33
```

```
user@host> show system services dhcp conflict
```

```
Detection time Detection method Address
2004-08-03 19:04:00 PDT ARP 3.3.3.5
2004-08-04 04:23:12 PDT Ping 4.4.4.8
2004-08-05 21:06:44 PDT Client 3.3.3.10
```

### Verifying DHCP Server Operation

**Purpose** Verify that the DHCP server operation has been configured.

**Action** From operational mode, enter these commands:

- **ping** command to verify that a client responds to ping packets containing the destination IP address assigned by the device.
- **ipconfig /all** command to display the IP configuration on the client. For example, on a PC running Microsoft Windows, enter **ipconfig /all** at the command prompt to display the PC's IP configuration.

```
user@host> ping 192.168.2.2
```

```
PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=255 time=8.856 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=255 time=11.543 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=255 time=10.315 ms
...
```

```
C:\Documents and Settings\user> ipconfig /all
```

Windows 2000 IP Configuration

```
Host Name : my-pc
Primary DNS Suffix : mycompany.net
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : mycompany.net mylab.net
```

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix . : mycompany.net mylab.net
Description : 10/100 LAN Fast Ethernet Card
Physical Address. : 02-04-06-08-0A-0C
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.2.2
Subnet Mask : 255.255.254.0
Default Gateway : 192.168.10.3
DHCP Server : 192.168.2.1
DNS Servers : 192.168.10.2
Primary WINS Server : 192.168.10.4
```

```

Secondary WINS Server : 192.168.10.5
Lease Obtained. : Monday, January 24, 2005 8:48:59 AM
Lease Expires : Monday, February 7, 2005 8:48:59 AM

```

**Related  
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
- [Understanding DHCP Server Operation on page 922](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)
- [DHCP Settings and Restrictions Overview on page 921](#)

## Configuring a DHCP Client

- [Understanding DHCP Client Operation on page 935](#)
- [Minimum DHCP Client Configuration on page 935](#)
- [Configuring DHCP Client-Specific Attributes for Address-Assignment Pools on page 936](#)
- [Configuring Optional DHCP Client Attributes on page 937](#)
- [Verifying and Managing DHCP Client Configuration on page 937](#)
- [Example: Configuring the Device as a DHCP Client on page 938](#)

## 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 920](#)
- [Example: Configuring the Device as a DHCP Client on page 938](#)
- [Understanding DHCP Relay Agent Operation on page 943](#)
- [DHCP Settings and Restrictions Overview on page 921](#)

## 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 937](#)

## 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.net

```



**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 926](#)

## 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 935](#)

## 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**
- [Example: Configuring the Device as a DHCP Client on page 938](#)

## Example: Configuring the Device as a DHCP Client

This example shows how to configure the device as a DHCP client.

- [Requirements on page 938](#)
- [Overview on page 939](#)
- [Configuration on page 939](#)
- [Verification on page 941](#)

### Requirements

---

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.



## Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

## Configuration

- [\[xref target has no title\]](#)

### 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, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet dhcp
set interfaces ge-0/0/1 unit 0 family inet dhcp client-identifier 00:0a:12:00:12:12
set interfaces ge-0/0/1 unit 0 family inet dhcp options no-hostname
set interfaces ge-0/0/1 unit 0 family inet dhcp lease-time 86400
set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-attempt 6
set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-interval 5
set interfaces ge-0/0/1 unit 0 family inet dhcp server-address 10.1.1.1
set interfaces ge-0/0/1 unit 0 family inet dhcp vendor-id ether
```

### GUI Step-by-Step Procedure

To configure the device as a DHCP client:

1. In the J-Web user interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Under Interfaces, click **ge-0/0/1**.
3. Under Unit, next to the unit number, click **Edit**.
4. Under Family, select the **Inet** check box and click **Edit**.
5. Next to Dhcp, click **Yes** and click **Configure**.
6. Configure the DHCP client identifier as either an ASCII or hexadecimal value. Next to Client identifier, click **Configure**.
7. From the Client identifier choice list, select **hexadecimal**.
8. In the Hexadecimal box, type the client identifier—**00:0a:12:00:12:12**.
9. Click **OK**.
10. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).

11. Set the DHCP lease time in seconds. From the Lease time list, select **Enter Specific Value**.
12. In the Length box, type **86400**.
13. Set the retransmission number of attempts. In the Retransmission attempt box, type **6**.
14. Set the retransmission interval in seconds. In the Retransmission interval box, type **5**.
15. Set the IPv4 address of the preferred DHCP server. In the Server address box, type **10.1.1.1**.
16. Set the vendor class ID. In the Vendor id box, type **ether**.
17. Click **OK**.
18. Click **OK** to check your configuration and save it as a candidate configuration.
19. 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* in the *CLI User Guide*.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.  

```
[edit]
user@host# edit interfaces ge-0/0/1 unit 0 family inet dhcp
```
2. Configure the DHCP client identifier as a hexadecimal value.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set client-identifier 00:0a:12:00:12:12
```
3. Configure options no-hostname if you do not want the client to send the hostname in packets.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set options no-hostname
```
4. Set the DHCP lease time.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set lease-time 86400
```
5. Set the number of attempts allowed to retransmit a DHCP packet.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set retransmission-attempt 6
```
6. 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]
user@host# set retransmission-interval 5
```
7. Set the IPv4 address of the preferred DHCP server.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
```

```
user@host# set server-address 10.1.1.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]
user@host# set vendor-id ether
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces ge-0/0/1 unit 0 family inet** 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 ge-0/0/1 unit 0 family inet
dhcp {
 client-identifier hexadecimal 00:0a:12:00:12:12;
 options no-hostname;
 lease-time 86400;
 retransmission-attempt 6;
 retransmission-interval 5;
 server-address 10.1.1.1;
 update-server;
 vendor-id ether;
}
```

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

### Verification

Confirm that the configuration is working properly.

- [Verifying the DHCP Client on page 941](#)

#### *Verifying the DHCP Client*

**Purpose** Verify that the DHCP client information has been configured.

**Action** From operational mode, enter these commands:

- **show system services dhcp client** command to display DHCP client information.
- **show system services dhcp client *interface-name*** command to display more information about a specific interface.
- **show system services dhcp client statistics** command to show client statistics.

These commands produce the following sample output:

```
user@host> show system services dhcp client

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
update server enables
Lease Obtained at 2006-08-24 18:13:04 PST
Lease Expires at 2006-08-25 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: domain-name, Value: netscreen-50
```

```
user@host> show system services dhcp client ge-0/0/1.0
```

```
Logical Interface Name ge-0/0/1.0
Hardware address 00:12:1e:a9:7b:81
Client Status bound
Address obtained 30.1.1.20
update server enables
Lease Obtained at 2007-05-10 18:16:04 PST
Lease Expires at 2007-05-11 18:16:04 PST
```

```
DHCP Options:
Name: name-server, Value: [30.1.1.2]
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [77.77.77.77, 55.55.55.55]
Name: domain-name, Value: mylab.example.net
```

```
user@host> show system services dhcp client statistics
```

```
Packets dropped:
Total 0
Messages Received:
DHCP OFFER 0
DHCP ACK 8
DHCP NAK 0

Messages Sent:
DHCP DECLINE 0
DHCP DISCOVER 0
DHCP REQUEST 1
DHCP INFORM 0
DHCP RELEASE 0
DHCP RENEW 7
DHCP REBIND 0
```

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
  - [Understanding DHCP Server Operation on page 922](#)
  - [Understanding DHCP Client Operation on page 935](#)
  - [DHCP Settings and Restrictions Overview on page 921](#)

---

## Configuring a DHCP Relay Agent

- [Understanding DHCP Relay Agent Operation on page 943](#)
- [Minimum DHCP Relay Agent Configuration on page 943](#)

- [Verifying and Managing DHCP Relay Configuration on page 944](#)
- [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 944](#)

## 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.

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 relay operations are supported on all SRX Series devices in chassis cluster mode.

### Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
- [Understanding DHCP Server Operation on page 922](#)
- [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 944](#)
- [DHCP Settings and Restrictions Overview on page 921](#)

## 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 1.1.1.1. 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 {
 1.1.1.1;
 }
 }
 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 944](#)

## 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 943](#)

## Example: Configuring the Device as a BOOTP or DHCP Relay Agent

This example shows how to configure the device as a BOOTP or DHCP relay agent.

- [Requirements on page 944](#)
- [Overview on page 945](#)
- [Configuration on page 945](#)
- [Verification on page 948](#)

### Requirements

---

No special configuration beyond device initialization is required before configuring this feature.

## Overview

In this example, you enable the DHCP relay agent to relay BOOTP or DHCP messages to a BOOTP server. You enable VPN encryption to allow client requests to pass through the VPN tunnel. You specify the IP time-to-live value to be set in responses to the client as 20. The range is from 1 through 255. You then set the maximum number of hops allowed per packet to 10. The range is from 4 through 16.

Then you specify the minimum number of seconds before requests are forwarded as 300. The range is from 0 through 30,000 seconds. You set the description of the server (the value is a string), and you specify a valid server name or address to the server to forward (the value is an IPv4 address). You define the routing instance, whose value is a nonreserved text string of 128 or fewer characters. You then specify the incoming BOOTP or DHCP request forwarding interface as ge-0/0/0. You enable the broadcast option if the Layer 2 interface is unknown.

You then specify the IP time-to-live value to be set in responses to the client as 30. The range is from 1 through 255. You set the description of the server as text and the DHCP option as 82. You set the maximum number of hops allowed per packet to 20 and specify the minimum number of seconds as 400 before requests are forwarded. You enable the no listen option. Finally, you enable VPN encryption to allow client requests to pass through the VPN tunnel.

## 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, and then enter **commit** from configuration mode.

```
set forwarding-options helpers bootp relay agent-option
set forwarding-options helpers bootp vpn
set forwarding-options helpers bootp client-response-ttl 20
set forwarding-options helpers bootp maximum-hop-count 10
set forwarding-options helpers bootp minimum-wait-time 300
set forwarding-options helpers bootp description text
set forwarding-options helpers bootp server 2.2.2.2
set forwarding-options helpers bootp server 2.2.2.2 routing instance rt-i-1
set forwarding-options helpers bootp interface ge-0/0/0
set forwarding-options helpers bootp interface ge-0/0/0 broadcast
set forwarding-options helpers bootp interface ge-0/0/0 client-response-ttl 30
set forwarding-options helpers bootp interface ge-0/0/0 description text
set forwarding-options helpers bootp interface ge-0/0/0 dhcp-option82
set forwarding-options helpers bootp interface ge-0/0/0 maximum-hop-count 20
set forwarding-options helpers bootp interface ge-0/0/0 minimum-wait-time 400
set forwarding-options helpers bootp interface ge-0/0/0 no-listen
set forwarding-options helpers bootp interface ge-0/0/0 vpn
```

### GUI Step-by-Step Procedure

To configure the device as a BOOTP/DHCP relay agent:

1. In the J-Web user interface, select **Configure>Services>DHCP>Boot DHCP Relay**.
2. Select the DHCP relay agent check box to enable the BOOTP/DHCP relay agent.

3. Select the VPN encryption check box.
4. In the Client response TTL box, type **20**.
5. In the Maximum hop count box, type **10**.
6. In the Minimum wait time box, type **300**.
7. In the Description box, type the description of the server.
8. Add a new server. Next to Server, click **Add new Entry**.
9. Next to the Name box, type **2.2.2.2**.
10. Define the routing instance. Next to Routing instance, click **Add new entry**.
11. In the Name box, type **rt-i-1** and click **OK**. A routing instance is optional.
12. Add a new interface. Next to Interface, click **Add new entry**.
13. In the Interface name box, type the interface name. For example, type **ge-0/0/0**.
14. In the Client response TTL box, type **30**.
15. In the Description box, type the description of the server.
16. Select the **Dhcp option 82** check box.
17. In the Maximum hop count box, type **20**.
18. In the Minimum wait time box, type **400**.
19. Select the **No listen** check box.
20. Select the **VPN encryption** check box.
21. Click **OK** until you return to the Configuration page.
22. Click **OK** to check your configuration and save it as a candidate configuration.
23. 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* in the *CLI User Guide*.

To configure the device as a BOOTP or DHCP relay agent:

1. Set the DHCP relay agent.  

```
[edit]
user@host# edit forwarding-options helpers bootp
user@host# set relay agent-option
```
2. Enable VPN encryption to allow client requests to pass through VPN tunnel.  

```
[edit forwarding-options helpers bootp]
user@host# set vpn
```
3. Set the IP time-to-live value. .  

```
[edit forwarding-options helpers bootp]
user@host# set client-response-ttl 20
```



4. Set the maximum number of hops allowed per packet.  

```
[edit forwarding-options helpers bootp]
user@host# set maximum-hop-count 10
```
5. Set the minimum wait time in seconds.  

```
[edit forwarding-options helpers bootp]
user@host# set minimum-wait-time 300
```
6. Specify the description of the server.  

```
[edit forwarding-options helpers bootp]
user@host# set description text
```
7. Add a new server.  

```
[edit forwarding-options helpers bootp]
user@host# set server 2.2.2.2
```
8. Define the routing instance.  

```
[edit forwarding-options helpers bootp]
user@host# set server 2.2.2.2 routing-instance rt-i-1
```
9. Define the incoming BootP request forwarding interface.  

```
[edit forwarding-options helpers bootp]
user@host# set interface ge-0/0/0
```
10. Enable broadcast option.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set broadcast
```
11. Define the IP time-to-live value.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set client-response-ttl 30
```
12. Specify the description of the server.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set description text
```
13. Set the DHCP option 82.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set dhcp-option82
```
14. Specify the maximum number of hops allowed per packet.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set forwarding-options helpers bootp interface ge-0/0/0
maximum-hop-count 20
```
15. Set the minimum wait time.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set minimum-wait-time 400
```
16. Set the no listen option.  

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set no-listen
```

17. Enable VPN encryption to allow client requests to pass through the VPN tunnel.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set vpn
```

**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
helpers {
 bootp {
 relay-agent-option;
 description text;
 server 2.2.2.2 routing-instance rt-i-1;
 maximum-hop-count 10;
 minimum-wait-time 300;
 client-response-ttl 20;
 vpn;
 }
 interface {
 ge-0/0/0 {
 no-listen;
 broadcast;
 description text;
 maximum-hop-count 20;
 minimum-wait-time 400;
 client-response-ttl 30;
 vpn;
 dhcp-option82;
 }
 }
}
```

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

---

### Verification

Confirm that the configuration is working properly.

#### *Verifying DHCP Relay Statistics*

**Purpose** Verify that the DHCP Relay statistics have been configured.

**Action** From operational mode, enter the **show system services dhcp relay-statistics** command.

```
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
```

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 920](#)
  - [Understanding DHCP Relay Agent Operation on page 943](#)
  - [DHCP Settings and Restrictions Overview on page 921](#)

## Configuring a DHCPv6 Local Server

- [DHCPv6 Server Overview on page 949](#)
- [Creating a Security Policy for DHCPv6 on page 950](#)
- [Example: Configuring DHCPv6 Server Options on page 950](#)
- [Example: Configuring an Address-Assignment Pool on page 953](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 955](#)
- [Configuring Address-Assignment Pool Linking on page 956](#)
- [Configuring DHCP Client-Specific Attributes on page 956](#)
- [Configuring an Address-Assignment Pool for Router Advertisement on page 957](#)
- [Understanding DHCPv6 Client and Server Identification on page 958](#)

## 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 950](#)
- [Example: Configuring an Address-Assignment Pool on page 953](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 955](#)
- [Creating a Security Policy for DHCPv6 on page 950](#)

## 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 3000:1.

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 949](#)
- [Example: Configuring DHCPv6 Server Options on page 950](#)
- [Example: Configuring an Address-Assignment Pool on page 953](#)

## Example: Configuring DHCPv6 Server Options

This example shows how to configure DHCPv6 server options.

- [Requirements on page 951](#)
- [Overview on page 951](#)

- [Configuration on page 951](#)
- [Verification on page 953](#)

## 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 3000::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, and then 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 3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 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* 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 3000::1/64

```
 7. Set router advertisement for the interface.


```

[edit protocols]
user@host# set router-advertisement interface ge-0/0/3.0 prefix 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 3000::1/64;
  }
}

```

```
[edit]
user@host# show protocols
router-advertisement {
  interface ge-0/0/3.0 {
    prefix 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 949 • Example: Configuring an Address-Assignment Pool on page 953 • Configuring a Named Address Range for Dynamic Address Assignment on page 955 • Creating a Security Policy for DHCPv6 on page 950 |

Example: Configuring an Address-Assignment Pool

This example shows how to configure an address-assignment pool.

- [Requirements on page 953](#)
- [Overview on page 954](#)
- [Configuration on page 954](#)
- [Verification on page 955](#)

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 `3000:0000::/10`, the range name as `range1`, and the IPv6 range for DHCPv6 clients from a low of `3000:0000::/32` to a high of `3000:1000::/32`. 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 `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, and then 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 3000:0000::/10
set access address-assignment pool my-pool family inet6 range range1 low
  3000:0000::/32 high 3000:1000::/32
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
  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* 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 3000:0000::/10
user@host# set range range1 low 3000:0000::/32 high 3000:1000::/32
```
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 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 3000:0000::/10;
    range range1 {
      low 3000:0000::/32;
      high 3000:1000::/32;
    }
    dhcp-attributes {
      maximum-lease-time 120;
      grace-period 3600;
      dns-server {
        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 949](#)
 - [Example: Configuring DHCPv6 Server Options on page 950](#)
 - [Configuring a Named Address Range for Dynamic Address Assignment on page 955](#)
 - [Creating a Security Policy for DHCPv6 on page 950](#)

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 3000:5000::/10
user@host# set range range2 low 3000:2000::/32 high 3000:3000::/32
```

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 956](#)

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 927](#)

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 97 on page 957](#) describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 97: 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 955](#)

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 955](#)

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 959](#)

Configuring a DHCPv6 Client

- [DHCPv6 Client Overview on page 959](#)
- [Minimum DHCPv6 Client Configuration on page 960](#)
- [Configuring Optional DHCPv6 Client Attributes on page 961](#)
- [Configuring Nontemporary Address Assignment on page 962](#)
- [Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation on page 962](#)
- [Configuring Auto-Prefix Delegation on page 963](#)
- [Configuring the DHCPv6 Client Rapid Commit Option on page 964](#)

- [Configuring a DHCPv6 Client in Autoconfig Mode on page 964](#)
- [Configuring TCP/IP Propagation on a DHCPv6 Client on page 965](#)

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 960](#)

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 959](#)

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 960](#)

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 960](#)

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 960](#)

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 960](#)
- [Configuring Optional DHCPv6 Client Attributes on page 961](#)

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 959](#)

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 960](#)
- [Configuring Optional DHCPv6 Client Attributes on page 961](#)

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 959](#)
- [Minimum DHCPv6 Client Configuration on page 960](#)

Configuring DHCP in Chassis Cluster Mode

- [Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode on page 965](#)
- [Example: Configuring the Device as a DHCP Client in Chassis Cluster Mode on page 970](#)

Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode

This example shows how to configure a DHCP server in chassis cluster mode.

- [Requirements on page 966](#)
- [Overview on page 966](#)
- [Configuration on page 966](#)
- [Verification on page 969](#)

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP servers
- One SRX Series device as DHCP client
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP servers and a third SRX Series device as a DHCP client. Configure the two DHCP servers in chassis cluster mode.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as `g1` and enable the DHCP local server on interface `reth1`.

For the DHCP client, you specify the interface as `ge-0/0/1`, set the logical unit as `0`, and create a DHCP inet family. You then specify the DHCP client identifier as `00:0a:12:00:12:12` in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

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.

Configure DHCP Server 1 and Server 2:

```
set system services dhcp-local-server group g1 interface reth1
set access address-assignment pool p1 family inet network 1.1.1.1/10
set access address-assignment pool p1 family inet range r1 low 1.1.1.5
set access address-assignment pool p1 family inet range r1 high 1.1.1.20
```

Configure chassis cluster on DHCP Server 1 and DHCP Server 2:

```
set chassis cluster reth-count 4
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 2000
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-6/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.1.1.1/24
```

Configure the DHCP client:

```
set interfaces ge-0/0/1 unit 0 family inet dhcp-client
set interfaces ge-0/0/1 unit 0 family inet dhcp-client client-identifier user-id ascii
00:0a:12:00:12:12
set interfaces ge-0/0/1 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/1 unit 0 family inet dhcp-client server-address 10.1.1.1
set interfaces ge-0/0/1 unit 0 family inet dhcp-client vendor-id ether
```

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* in the *CLI User Guide*.

To configure the devices as DHCP servers:

1. Configure the DHCP local server.

```
[edit system services]
user@host# set dhcp-local-server group g1 interface reth1
```
2. Configure an address pool.

```
[edit access]
user@host# set address-assignment pool p1 family inet network 1.1.1.1/10
user@host# set address-assignment pool p1 family inet range r1 low 1.1.1.5
user@host# set address-assignment pool p1 family inet range r1 high 1.1.1.20
```

Step-by-Step Procedure

To configure the DHCP servers in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 4
```
2. Enable control link recovery.

```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```
3. Configure heartbeat settings.

```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 2000
```
4. Configure the redundancy groups.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 0 node 0 priority 200
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

5. Configure redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces ge-6/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
user@host# set interfaces reth1 unit 0 family inet address 10.1.1.1/24
```

Step-by-Step Procedure

To configure the device as DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/1 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```

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 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
```

Results From configuration mode, confirm your configuration by entering the **show** 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 {
  group g1 {
    interface reth1.0;
  }
}
```

```

}

[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
        network 1.1.1.1/10;
        range r1 {
            low 1.1.1.5;
            high 1.1.1.20;
        }
    }
}

[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 4;
heartbeat-interval 2000;
redundancy-group 0 {
    node 0 priority 200;
    node 1 priority 1;
}

[edit]
user@host# show interfaces reth1
redundant-ether-options {
    redundancy-group 1;
}
unit 0 {
    family inet {
        address 10.1.1.24;
    }
}

[edit]
user@host# show interfaces ge-0/0/1 unit 0 family inet
dhcp-client {
    client-identifier user-id ascii 00:0a:12:00:12:12;
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    server-address 10.1.1.1;
    vendor-id ether;
}

```

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

Verification

Verifying the DHCP Server in Chassis Cluster Mode

Purpose Verify that the DHCP server is working in chassis cluster mode.

Action From operational mode, enter the **show dhcp server binding** and **show dhcp server statistics** commands.

```

user@host> show dhcp server binding

IP address      Session Id  Hardware address  Expires  State  Interface
10.1.1.1        1          64:87:88:79:a3:81  81855    BOUND  reth1

user@host> show dhcp server statistics

Packets dropped:
  Total          0
  dhcp-service total 0

Messages received:
  BOOTREQUEST    2
  DHCPDECLINE    0
  DHCPDISCOVER   1
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    1

Messages sent:
  BOOTREPLY      2
  DHCPOFFER      1
  DHCPACK        0
  DHCPNAK        0
  DHCPFORCERENEW 0

```

Meaning The sample output shows that DHCP servers configured in the example work in a chassis cluster.

Related Documentation

- [Understanding DHCP Server Operation on page 922](#)
- [Example: Configuring the Device as a DHCP Server on page 929](#)

Example: Configuring the Device as a DHCP Client in Chassis Cluster Mode

This example shows how to configure the device as a DHCP client in chassis cluster mode.

- [Requirements on page 970](#)
- [Overview on page 971](#)
- [Configuration on page 971](#)
- [Verification on page 974](#)

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP client
- One SRX Series device as DHCP server
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server. Configure the two DHCP clients in chassis cluster mode.

For DHCP clients, you specify the interface as `reth1`, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as `00:0a:12:00:12:12` in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options `no-hostname` if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds. You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 1.1.1.1 and the vendor class ID to ether.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as `g1` and enable the DHCP local server on interface `ge-0/0/2.0`.

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, and then enter **commit** from configuration mode.

Configure DHCP Client 1 and Client 2:

```
set interfaces reth1 unit 0 family inet dhcp-client
set interfaces reth1 unit 0 family inet dhcp-client client-identifier user-id ascii
  00:0a:12:00:12:12
set interfaces reth1 unit 0 family inet dhcp-client options no-hostname
set interfaces reth1 unit 0 family inet dhcp-client lease-time 86400
set interfaces reth1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces reth1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces reth1 unit 0 family inet dhcp-client server-address 1.1.1.1
set interfaces reth1 unit 0 family inet dhcp-client vendor-id ether
```

Configure chassis cluster on Client 1 and Client 2:

```
set chassis cluster reth-count 2
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 1000
```

```

set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-4/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1

```

Configure the DHCP server:

```

set system service dhcp-local-server group g1 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set access address-assignment pool p1 family inet network 1.1.1.0/24
set access address-assignment pool p1 family inet range r1 low 1.1.1.5
set access address-assignment pool p1 family inet range r1 high 1.1.1.20

```

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* in the *CLI User Guide*.

To configure the devices as DHCP clients:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces reth1 unit 0 family inet dhcp-client
```
2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```
3. Set the hostname if you do not want the DHCP client to send hostname in the packets (RFC option code 12).

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```
4. Set the DHCP lease time.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```
5. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```
6. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```
7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set server-address 1.1.1.1
```
8. Set the vendor class ID for the DHCP client.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

Step-by-Step Procedure

To configure the DHCP clients in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.


```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 2
```
2. Enable control link recovery.


```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```
3. Configure heartbeat settings.


```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 1000
```
4. Configure the redundancy groups.


```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 node 0 priority 100
user@host# set chassis cluster redundancy-group 1 node 1 priority 1
user@host# set chassis cluster redundancy-group 0 node 0 priority 100
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```
5. Configure redundant Ethernet interfaces.


```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
```

Step-by-Step Procedure

To configure the device as DHCP server:

1. Configure the DHCP local server.


```
[edit system services]
user@host# set dhcp-local-server group g1 interface ge-0/0/2.0
```
2. Configure IP address of the server.


```
[edit interfaces]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
```
3. Configure an address pool.


```
[edit access]
user@host# set address-assignment pool p1 family inet network 1.1.1.0/24
user@host# set address-assignment pool p1 family inet range r1 low 1.1.1.5
user@host# set address-assignment pool p1 family inet range r1 high 1.1.1.20
```

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

```
[edit]
user@host# show interfaces reth1 unit 0 family inet
```

```
dhcp-client {
  client-identifier user-id ascii 00:0a:12:00:12:12;
  options no-hostname;
  lease-time 86400;
  retransmission-attempt 6;
  retransmission-interval 5;
  server-address 1.1.1.1;
  vendor-id ether;
}

[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 2;
heartbeat-interval 1000;
redundancy-group 0 {
  node 0 priority 100;
  node 1 priority 1;
}
redundancy-group 1 {
  node 0 priority 100;
  node 1 priority 1;
}

[edit]
user@host# show interfaces reth1
redundant-ether-options {
  redundancy-group 1;
}

[edit]
user@host# show access address-assignment
pool p1 {
  family inet {
    network 1.1.1.0/24;
    range r1 {
      low 1.1.1.5;
      high 1.1.1.20;
    }
  }
}
```

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

Verification

Confirm that the configuration is working properly.

- [Verifying the DHCP Client in Chassis Cluster Mode on page 974](#)

Verifying the DHCP Client in Chassis Cluster Mode

Purpose Verify that the DHCP client is working in chassis cluster mode.

Action From operational mode, enter the **show dhcp client binding**, **show dhcp client statistics** and **show dhcp client binding interface reth1 detail** commands.

```

user@host> show dhcp client binding

IP address      Hardware address Expires      State      Interface
1.1.1.14        00:1f:12:e3:34:01 84587       BOUND      reth1.0

user@host> show dhcp client statistics

Packets dropped:
  Total          4
  Send error     4

Messages received:
  BOOTREPLY      3
  DHCPPOFFER     1
  DHCPACK        2
  DHCPNAK        0
  DHCPFORCERENEW 0

Messages sent:
  BOOTREQUEST    0
  DHCPDECLINE    0
  DHCPDISCOVER   5
  DHCPREQUEST    8
  DHCPINFORM     0
  DHCPRELEASE    1
  DHCPRENEW      0
  DHCPREBIND     0

user@host> show dhcp client binding interface reth1 detail

Client Interface: reth1.0
  Hardware Address:      00:10:db:ff:10:01
  State:                 BOUND(LOCAL_CLIENT_STATE_BOUND)
  Lease Expires:         2013-12-18 10:15:36 CST
  Lease Expires in:      30 seconds
  Lease Start:           2013-12-17 10:15:36 CST
  Server Identifier:     1.1.1.1
  Client IP Address:     10.1.1.14
  Update Server          No

DHCP options:
  Name: dhcp-lease-time, Value: 1 day
  Name: server-identifier, Value: 10.1.1.1
  Name: subnet-mask, Value: 255.255.255.0

```

Meaning The sample output shows that DHCP clients configured in the example work in a chassis cluster.

Related Documentation

- [Understanding DHCP Client Operation on page 935](#)
- [Example: Configuring the Device as a DHCP Client on page 938](#)

CHAPTER 31

Managing System Files

- [Performing File Management Tasks on page 977](#)

Performing File Management Tasks

- [File Management Overview on page 977](#)
- [Decrypting Configuration Files on page 978](#)
- [Encrypting Configuration Files on page 978](#)
- [Modifying the Encryption Key on page 979](#)
- [Cleaning Up Files on page 980](#)
- [Cleaning Up Files with the CLI on page 981](#)
- [Deleting Files on page 982](#)
- [Deleting the Backup Software Image on page 982](#)
- [Downloading Files on page 983](#)
- [Configuring RADIUS System Accounting on page 983](#)
- [Managing Accounting Files on page 986](#)

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 on page 980](#)
- [Cleaning Up Files with the CLI on page 981](#)
- [Managing Accounting Files on page 986](#)
- [Encrypting Configuration Files on page 978](#)
- *Network Monitoring and Troubleshooting Guide for Security Devices*

- [Junos OS System Log Reference for Security Devices](#)

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

- [Network Monitoring and Troubleshooting Guide for Security Devices](#)

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 98 on page 978](#).



NOTE: The **request system set-encryption-key** command is not supported on high-end SRX devices, therefore, this task does not apply to such devices.

Table 98: request system set-encryption-key Commands

| CLI Command | Description |
|--|--|
| request system set-encryption-key | <p>Sets the encryption key and enables default configuration file encryption:</p> <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 98: 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 • *Network Monitoring and Troubleshooting Guide for Security Devices*

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

- *Network Monitoring and Troubleshooting Guide for Security Devices*

Cleaning Up Files

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**
- *Network Monitoring and Troubleshooting Guide for Security Devices*

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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

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 984](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 984](#)
3. [Configuring RADIUS Server Accounting on page 984](#)

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 or IPv6 address 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 $9$ABC123;
            source-address 10.1.1.1;
            retry 3;
            timeout 3;
          }
          10.6.6.6 secret $9$ABC123;
          10.7.7.7 secret $9$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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

CHAPTER 32

Working with Junos OS Licenses

- [Managing Junos OS Licenses on page 989](#)

Managing Junos OS Licenses

- [Junos OS Feature License Keys on page 989](#)
- [Software Feature Licenses for SRX Series Devices on page 991](#)
- [Displaying License Keys in J-Web on page 1000](#)
- [Downloading License Keys on page 1001](#)
- [Generating a License Key on page 1001](#)
- [Saving License Keys on page 1002](#)
- [Updating License Keys on page 1003](#)
- [Example: Adding a New License Key on page 1003](#)
- [Example: Deleting a License Key on page 1006](#)

Junos OS Feature License Keys

This section contains the following topics:

- [License Key Components on page 989](#)
- [License Management Fields Summary on page 990](#)

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 29 on page 197](#).

Table 99: 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 209](#)
 - [Updating License Keys on page 210](#)

- [Saving License Keys on page 210](#)
- [Downloading License Keys on page 209](#)

Software Feature Licenses for SRX Series Devices

Table 100: Junos OS Feature Licenses

| Junos OS License Requirements | | | | | | | | | | |
|--|--------|--------|--------|--------|--------|--------|--------|---------|--------------|--------------|
| Feature | SRX100 | SRX110 | SRX210 | SRX220 | SRX240 | SRX550 | SRX650 | SRX1400 | SRX3000 line | SRX5000 line |
| Access Manager | X | X | X | X | X | X | X | | | |
| BGP Route Reflectors | | | | | | | X | | | |
| Dynamic VPN | X | X | X | X | X | X | X | | | |
| IDP Signature Update* | X * | X | X * | X * | X * | X | X | X | X | X |
| Application Signature Update (Application Identification)* | X | X | X | X | X | X | X | X | X | X |
| Juniper-Kaspersky Antivirus* | X | X | X | X | X | X | X | | | |
| Juniper-Sophos Antivirus* | X | X | X | X | X | X | X | X | X | X |
| Juniper-Sophos Antispam* | X | X | X | X | X | X | X | X | X | X |
| Juniper-Enhanced Web filtering* | X | X | X | X | X | X | X | X | X | X |
| Juniper-Websense Web filtering* | X | X | X | X | X | X | X | | | |
| Logical Systems | | | | | | | | X | X | X |
| SRX100 Memory Upgrade | X | | | | | | | | | |

* Indicates support on high-memory devices only.

[Table 31 on page 200](#) 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 101: 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) | SRX100 | SRX100-APPSEC-A-1 |
| | | SRX100-APPSEC-A-3 |
| | | SRX100-APPSEC-A-5 |
| | SRX210, SRX220, and SRX240 | SRX2XX-APPSEC-A-1 |
| | | SRX2XX-APPSEC-A-3 |
| | | SRX2XX-APPSEC-A-5 |
| | SRX550 | SRX550-APPSEC-A-1 |
| | | SRX550-APPSEC-A-3 |
| | | SRX550-APPSEC-A-5 |
| | SRX650 | SRX650-APPSEC-A-1 |
| | | SRX650-APPSEC-A-3 |
| | | SRX650-APPSEC-A-5 |
| | SRX1400 | SRX1400-APPSEC-A-1 |
| | | SRX1400-APPSEC-A-3 |
| | | SRX1400-APPSEC-A-1-R |
| | | SRX1400-APPSEC-A-3-R |
| | SRX3400 | SRX3400-APPSEC-A-1 |
| | | SRX3400-APPSEC-A-3 |
| | SRX3600 | SRX3600-APPSEC-A-1 |
| | | SRX3600-APPSEC-A-3 |
| | SRX5400 | SRX5400-APPSEC-1 |
| | | SRX5400-APPSEC-3 |
| | | SRX5400-APPSEC-5 |
| | SRX5600 | SRX5600-APPSEC-A-1 |
| | | SRX5600-APPSEC-A-3 |
| | | SRX5600-APPSEC-A-5 |
| | SRX5800 | |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|--|---------------------------|--------------------|
| IDP updates (1 year, 3 years, and 5 years) | SRX100, SRX110 | SRX5800-APPSEC-A-1 |
| | | SRX5800-APPSEC-A-3 |
| | | SRX5800-APPSEC-A-5 |
| | SRX100, SRX110 | SRX1XX-IDP |
| | | SRX1XX-IDP-3 |
| | | SRX1XX-IDP-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-IDP |
| | | SRX2XX-IDP-3 |
| | | SRX2XX-IDP-5 |
| | SRX550 | SRX550-IDP |
| | | SRX550-IDP-3 |
| | | SRX550-IDP-5 |
| | SRX650 | SRX650-IDP |
| | | SRX650-IDP-3 |
| | | SRX650-IDP-5 |
| IDP subscription (1 year and 3 years) | SRX3400, SRX3600 | SRX3K-IDP |
| | | SRX3K-IDP-3 |
| | SRX5400, SRX5600, SRX5800 | SRX5K-IDP |
| | | SRX5K-IDP-3 |
| | | SRX5K-IDP-3-R |
| | | SRX5K-IDP-R |
| | SRX5400, SRX5600, SRX5800 | SRX5K-IDP |
| | | SRX5K-IDP-3 |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|--|------------------------|---------------|
| Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years) | SRX100, SRX110 | SRX1XX-K-AV |
| | | SRX1XX-K-AV-3 |
| | | SRX1XX-K-AV-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-K-AV |
| | | SRX2XX-K-AV-3 |
| | | SRX2XX-K-AV-5 |
| | SRX550 | SRX550-K-AV |
| | | SRX550-K-AV-3 |
| | | SRX550-K-AV-5 |
| | SRX650 | SRX650-K-AV |
| | | SRX650-K-AV-3 |
| | | SRX650-K-AV-5 |
| Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years) | SRX100, SRX110 | SRX1XX-S-AV |
| | | SRX1XX-S-AV-3 |
| | | SRX1XX-S-AV-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-S-AV |
| | | SRX2XX-S-AV-3 |
| | | SRX2XX-S-AV-5 |
| | SRX550 | SRX550-S-AV |
| | | SRX550-S-AV-3 |
| | | SRX550-S-AV-5 |
| | SRX650 | SRX650-S-AV |
| | | SRX650-S-AV-3 |
| | | SRX650-S-AV-5 |

Table 101: 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) | SRX1400 | SRX1400-S-AV-1 |
| | | SRX1400-S-AV-3 |
| | | SRX1400-S-AV-5 |
| | SRX3400 | SRX3400-S-AV-1 |
| | | SRX3400-S-AV-3 |
| | | SRX3400-S-AV-5 |
| | SRX3600 | SRX3600-S-AV-1 |
| | | SRX3600-S-AV-3 |
| | | SRX3600-S-AV-5 |
| | 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) | SRX100, SRX110 | SRX1XX-S2-AS |
| | | SRX1XX-S2-AS-3 |
| | | SRX1XX-S2-AS-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-S2-AS |
| | | SRX2XX-S2-AS-3 |
| | | SRX2XX-S2-AS-5 |
| | SRX550 | SRX550-S2-AS |
| | | SRX550-S2-AS-3 |
| | | SRX550-S2-AS-5 |
| | SRX650 | SRX650-S2-AS |
| | | SRX650-S2-AS-3 |
| | | SRX650-S2-AS-5 |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|--|------------------------|----------------|
| Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years) | SRX1400 | SRX1400-S-AV-1 |
| | | SRX1400-S-AV-3 |
| | | SRX1400-S-AV-5 |
| | SRX3400 | SRX3400-S-AV-1 |
| | | SRX3400-S-AV-3 |
| | | SRX3400-S-AV-5 |
| | SRX3600 | SRX3600-S-AV-1 |
| | | SRX3600-S-AV-3 |
| | | SRX3600-S-AV-5 |
| | 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) | SRX100, SRX110 | SRX1XX-W-EWF |
| | | SRX1XX-W-EWF-3 |
| | | SRX1XX-W-EWF-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-W-EWF |
| | | SRX2XX-W-EWF-3 |
| | | SRX2XX-W-EWF-5 |
| | SRX550 | SRX550-W-EWF |
| | | SRX550-W-EWF-3 |
| | | SRX550-W-EWF-5 |
| | SRX650 | SRX650-W-EWF |
| | | SRX650-W-EWF-3 |
| | | SRX650-W-EWF-5 |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|---|------------------------|------------------|
| Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years) | SRX1400 | SRX1400-W-EWF-1 |
| | | SRX1400-W-EWF-3 |
| | | SRX1400-W-EWF-5 |
| | SRX3400 | SRX3400-W-EWF-1 |
| | | SRX3400-W-EWF-3 |
| | | SRX3400-W-EWF-5 |
| | SRX3600 | SRX3600-W-EWF-1 |
| | | SRX3600-W-EWF-3 |
| | | SRX3600-W-EWF-5 |
| | 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) | SRX100, SRX110 | SRX1XX-SMB4-CS |
| | | SRX1XX-SMB4-CS-3 |
| | | SRX1XX-SMB4-CS-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-SMB4-CS |
| | | SRX2XX-SMB4-CS-3 |
| | | SRX2XX-SMB4-CS-5 |
| | SRX550 | SRX550-SMB4-CS |
| | | SRX550-SMB4-CS-3 |
| | | SRX550-SMB4-CS-5 |
| | SRX650 | SRX650-SMB4-CS |
| | | SRX650-SMB4-CS-3 |
| | | SRX650-SMB4-CS-5 |

Table 101: 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) | SRX100, SRX110 | SRX1XX-S-SMB4-CS |
| | | SRX1XX-S-SMB4-CS-3 |
| | | SRX1XX-S-SMB4-CS-5 |
| | SRX210, SRX220, SRX240 | SRX2XX-S-SMB4-CS |
| | | SRX2XX-S-SMB4-CS-3 |
| | | SRX2XX-S-SMB4-CS-5 |
| | SRX550 | SRX550-S-SMB4-CS |
| | | SRX550-S-SMB4-CS-3 |
| | | SRX550-S-SMB4-CS-5 |
| | SRX650 | SRX650-S-SMB4-CS |
| | | SRX650-S-SMB4-CS-3 |
| | | SRX650-S-SMB4-CS-5 |
| Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years) | SRX1400 | SRX1400-CS-BUN-1 |
| | | SRX1400-CS-BUN-3 |
| | | SRX1400-CS-BUN-5 |
| | SRX3400 | SRX3400-CS-BUN-1 |
| | | SRX3400-CS-BUN-3 |
| | | SRX3400-CS-BUN-5 |
| | SRX3600 | SRX3600-CS-BUN-1 |
| | | SRX3600-CS-BUN-3 |
| | | SRX3600-CS-BUN-5 |
| | 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 |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|---|--|------------------------|
| Dynamic VPN Client (5, 10, and 25 simultaneous users) | SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 | SRX-RAC-5-LTU |
| | | SRX-RAC-10-LTU |
| | | SRX-RAC-25-LTU |
| Dynamic VPN Service (5, 10, 25, and 50 simultaneous users) | SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550 | SRX-RAC-5-LTU |
| | SRX210, SRX240, SRX100, SRX220, SRX650, SRX110, SRX550 | SRX-RAC-10-LTU |
| | SRX210, SRX240, SRX100, SRX220, SRX650, SRX550 | SRX-RAC-25-LTU |
| | SRX240, SRX650, SRX220, SRX210, SRX550 | SRX-RAC-50-LTU |
| Dynamic VPN Service (100 and 150 simultaneous users) | SRX650, SRX220, SRX240, SRX550 | SRX-RAC-100-LTU |
| | | SRX-RAC-150-LTU |
| Dynamic VPN Service (250 simultaneous users) | SRX650, SRX240, SRX550
NOTE: Requires Junos OS 11.2R3 or later | SRX-RAC-250-LTU |
| Dynamic VPN Service (500 simultaneous users) | SRX650, SRX550
NOTE: Requires Junos OS 11.2R3 or later | SRX-RAC-500-LTU |
| Express Path License (formerly known as <i>services offloading</i>)

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. | SRX1400 | SRX1K-SVCS-OFFLOAD-RTU |
| | SRX3400, SRX3600 | SRX3K-SVCS-OFFLOAD-RTU |
| | SRX5400, SRX5600, SRX5800 | SRX5K-SVCS-OFFLOAD-RTU |
| Memory Software License (Upgrades SRX100B model from 512-MB RAM to 1-GB RAM) | SRX100 | SRX100-MEM-LIC-UPG |
| Advanced BGP License | SRX650 only | SRX-BGP-ADV-LTU |

Table 101: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|--|-------------------|------------------|
| Logical Systems License (incremental 1, 5, and 25 numbers) | SRX1400 | SRX-1400-LSYS-1 |
| | | SRX-1400-LSYS-25 |
| | | SRX-1400-LSYS-5 |
| | SRX3400 | SRX-3400-LSYS-1 |
| | | SRX-3400-LSYS-5 |
| | | SRX-3400-LSYS-25 |
| | SRX3600 | SRX-3600-LSYS-1 |
| | | SRX-3600-LSYS-5 |
| | | SRX-3600-LSYS-25 |
| | 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 |

- Related Documentation**
- [License Enforcement on page 196](#)
 - [Junos OS Feature License Keys on page 196](#)
 - [Working with License Keys for SRX Series Devices on page 209](#)

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 196](#)
- [Generating a License Key on page 209](#)
- [Example: Adding a New License Key on page 210](#)
- [Example: Deleting a License Key on page 213](#)
- [Downloading License Keys on page 209](#)

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 196](#)
- [Generating a License Key on page 209](#)
- [Example: Adding a New License Key on page 210](#)
- [Example: Deleting a License Key on page 213](#)

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 210](#)
 - [Example: Deleting a License Key on page 213](#)
 - [Updating License Keys on page 210](#)
 - [Downloading License Keys on page 209](#)

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 196](#)
 - [Generating a License Key on page 209](#)
 - [Example: Adding a New License Key on page 210](#)
 - [Example: Deleting a License Key on page 213](#)
 - [Downloading License Keys on page 209](#)

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 196](#)
- [Generating a License Key on page 209](#)
- [Example: Adding a New License Key on page 210](#)
- [Example: Deleting a License Key on page 213](#)
- [Downloading License Keys on page 209](#)

Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 1003](#)
- [Overview on page 1003](#)
- [Configuration on page 1004](#)
- [Verification on page 1005](#)

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 add a new license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

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.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

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.



NOTE: If you added the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a high-memory device.

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 on page 1005](#)
- [Verifying License Usage on page 1005](#)
- [Verifying Installed License Keys on page 1006](#)

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 196](#)
 - [Generating a License Key on page 209](#)
 - [Example: Deleting a License Key on page 213](#)
 - [Updating License Keys on page 210](#)
 - [Downloading License Keys on page 209](#)

Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 1006](#)
- [Overview on page 1006](#)
- [Configuration on page 1007](#)
- [Verification on page 1007](#)

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 delete a license key, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
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**.



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

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
```



NOTE: If you deleted the SRX100 Memory Upgrade license, the device reboots immediately and comes back up as a low-memory device.

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 1007](#)

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 209](#)
 - [Example: Adding a New License Key on page 210](#)
 - [Updating License Keys on page 210](#)
 - [Downloading License Keys on page 209](#)

CHAPTER 33

Configuration Statements and Operational Commands

- [Configuration Statements on page 1009](#)
- [Operational Commands on page 1160](#)

Configuration Statements

- [\[edit security certificates\] Hierarchy Level on page 1012](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 1012](#)
- [Interfaces Configuration Statement Hierarchy on page 1012](#)
- [Groups Configuration Statement Hierarchy on page 1028](#)
- [System Configuration Statement Hierarchy on page 1028](#)
- [address-assignment \(Access\) on page 1060](#)
- [address-pool \(Access\) on page 1063](#)
- [allow-configuration on page 1064](#)
- [allow-configuration-regexps on page 1065](#)
- [authentication-key on page 1066](#)
- [authentication-order on page 1067](#)
- [boot-server \(NTP\) on page 1068](#)
- [broadcast on page 1069](#)
- [broadcast-client on page 1070](#)
- [ciphers on page 1071](#)
- [connection-limit on page 1072](#)
- [client-ia-type on page 1073](#)
- [client-identifier \(dhcp-client\) on page 1073](#)
- [client-identifier \(dhcpv6-client\) on page 1074](#)
- [client-list-name \(SNMP\) on page 1074](#)
- [client-type on page 1075](#)
- [deny-configuration on page 1075](#)

- [deny-configuration-regexps](#) on page 1076
- [destination](#) (Accounting) on page 1077
- [dhcp-attributes](#) (Access IPv4 Address Pools) on page 1078
- [dhcp-attributes](#) (Access IPv6 Address Pools) on page 1080
- [dhcp-client](#) on page 1081
- [dhcp-local-server](#) (System Services) on page 1082
- [dhcpv6](#) (System Services) on page 1086
- [dhcpv6-client](#) on page 1089
- [disable](#) (System Services) on page 1090
- [dlv](#) on page 1090
- [family](#) (Security Forwarding Options) on page 1091
- [file](#) (System Logging) on page 1092
- [forwarding-options](#) (Security) on page 1095
- [group](#) (System Services DHCP) on page 1096
- [host](#) (SSH Known Hosts) on page 1099
- [hostkey-algorithm](#) on page 1100
- [interface](#) (System Services DHCP) on page 1101
- [interfaces](#) (ARP) on page 1102
- [interfaces](#) (Security Zones) on page 1103
- [interface-traceoptions](#) (System Services DHCP) on page 1104
- [internet-options](#) on page 1106
- [kernel-replication](#) (System) on page 1107
- [lease-time](#) (dhcp-client) on page 1107
- [location](#) on page 1108
- [lockout-period](#) on page 1109
- [macs](#) on page 1110
- [max-pre-authentication-packets](#) on page 1111
- [multicast-client](#) on page 1111
- [name-server](#) (Access) on page 1112
- [neighbor-discovery-router-advertisement](#) (Access) on page 1112
- [ntp](#) on page 1113
- [outbound-ssh](#) on page 1114
- [overrides](#) (System Services DHCP) on page 1116
- [peer](#) (NTP) on page 1117
- [prefix](#) on page 1118
- [profillerd](#) on page 1119
- [protocol-version](#) on page 1119

- [proxy](#) on page 1120
- [radius-options](#) on page 1121
- [radius-server](#) on page 1122
- [rapid-commit](#) on page 1123
- [reconfigure \(System Services DHCP\)](#) on page 1124
- [req-option](#) on page 1125
- [retransmission-attempt \(dhcp-client\)](#) on page 1126
- [retransmission-attempt \(dhcpv6-client\)](#) on page 1126
- [retransmission-interval \(dhcp-client\)](#) on page 1127
- [root-authentication](#) on page 1128
- [single-connection](#) on page 1129
- [server \(NTP\)](#) on page 1130
- [server-address \(dhcp-client\)](#) on page 1131
- [services \(System Services\)](#) on page 1132
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\)](#) on page 1137
- [ssh-known-hosts](#) on page 1138
- [static-subscribers](#) on page 1139
- [statistics-service](#) on page 1139
- [subscriber-management](#) on page 1140
- [subscriber-management-helper](#) on page 1141
- [tacplus](#) on page 1142
- [tacplus-options](#) on page 1143
- [tacplus-server](#) on page 1144
- [traceoptions \(Outbound SSH\)](#) on page 1146
- [traceoptions \(System Services DHCP\)](#) on page 1148
- [trusted-key](#) on page 1150
- [uac-service](#) on page 1151
- [update-router-advertisement](#) on page 1152
- [update-server \(dhcp-client\)](#) on page 1152
- [update-server \(dhcpv6-client\)](#) on page 1152
- [usb-control](#) on page 1153
- [use-interface](#) on page 1153
- [user-id](#) on page 1154
- [vendor-id](#) on page 1154
- [vpn \(Forwarding Options\)](#) on page 1155
- [watchdog](#) on page 1155

- [web-management](#) on page 1156
- [web-management \(System Services\)](#) on page 1157

[edit security certificates] Hierarchy Level

```
security {
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority profile-name {
      ca-name name;
      crt 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](#) on page 57
 - [Installation and Upgrade Guide for Security Devices](#)

[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](#) on page 57

Interfaces Configuration Statement Hierarchy

Use the statements in the **interfaces** configuration hierarchy to configure interfaces on the device.

```

interfaces {
  interface-name {
    accounting-profile name;
    clocking (external | internal);
    dce;
    description text;
    disable;
    e1-options {
      bert-algorithm algorithm;
      bert-error-rate rate;
      bert-period seconds;
      fcs (16 | 32);
      framing (g704 | g704-no-crc4 | unframed);
      idle-cycle-flag (flags | ones);
      invert-data data;
      loopback (local | remote);
      start-end-flag (shared | filler);
      timeslots time-slot-range;
    }
    e3-options {
      bert-algorithm algorithm;
      bert-error-rate rate;
      bert-period seconds;
      compatibility-mode {
        digital-link {
          substrate value;
        }
        kentrox {
          substrate value;
        }
        larscom;
      }
      fcs (16 | 32);
      framing (g.751 | g.832);
      idle-cycle-flag value;
      invert-data;
      loopback (local | remote);
      (no-payload-scrambler | payload-scrambler);
      (no-unframed | -unframed);
      start-end-flag (filler | shared);
    }
    encapsulation (ether-vpls-ppp | ethernet-bridge | ethernet-ccc | ethernet-tcc |
      ethernet-vpls | extended-frame-relay-ccc | extended-frame-relay-tcc |
      extended-vlan-bridge | extended-vlan-ccc | extended-vlan-tcc | extended-vlan-vpls
      | frame-relay-port-ccc | vlan-ccc | vlan-vpls);
    fastether-options {
      802.3ad interface-name {
        (backup | primary);
        lacp {
          port-priority port-number;
        }
      }
      (auto-negotiation | no-auto-negotiation);
      ignore-l3-incompletes;
      ingress-rate-limit rate;
      (loopback | no-loopback);
    }
  }
}

```

```
mpls {
  pop-all-labels {
    required-depth number;
  }
}
redundant-parent interface-name;
source-address-filter mac-address;
}
flexible-vlan-tagging;
gigether-options {
  802.3ad interface-name {
    (backup | primary);
    lacp {
      port-priority port-number;
    }
  }
}
(auto-negotiation <remote-fault> (local-interface-offline | local-interface-online)
 | no-auto-negotiation);
(flow-control | no-flow-control);
ignore-l3-incompletes;
(loopback | no-loopback);
mpls {
  pop-all-labels {
    required-depth [number];
  }
}
redundant-parent interface-name;
source-address-filter mac-address;
}
gratuitous-arp-reply;
hierarchical-scheduler {
  maximum-hierarchy-levels 2;
}
hold-time {
  down milliseconds;
  up milliseconds;
}
keepalives {
  down-count number;
  interval number;
  up-count number;
}
link-mode (full-duplex | half-duplex);
lmi {
  lmi-type (ansi | c-lmi | itu);
  n391dte number;
  n392dce number;
  n392dte number;
  n393dce number;
  n393dte number;
  t391dte number;
  t392dce number;
}
logical-tunnel-options {
  per-unit-mac-disable;
}
```

```
mac mac-address;
mtu bytes;
native-vlan-id vlan-id;
no-gratuitous-arp-request;
no-keepalives;
optics-options {
    alarm {
        low-light-alarm (link-down | syslog);
    }
    warning {
        low-light-warning (link-down | syslog);
    }
    wavelength wavelength-options;
}
otn-options {
    bytes {
        transmit-payload-type number;
    }
    fec (efec | gfec | none);
    (laser-enable | no-laser-enable);
    (line-loopback | no-line-loopback);
    rate (fixed-stuff-bytes | no-fixed-stuff-bytes | pass-thru);
    trigger {
        oc-lof {
            hold-time {
                down milliseconds;
                up milliseconds;
            }
            ignore;
        }
        oc-lom {
            hold-time {
                down milliseconds;
                up milliseconds;
            }
            ignore;
        }
        oc-los {
            hold-time {
                down milliseconds;
                up milliseconds;
            }
            ignore;
        }
        oc-wavelength-lock {
            hold-time {
                down milliseconds;
                up milliseconds;
            }
            ignore;
        }
        odu-ais {
            hold-time {
                down milliseconds;
                up milliseconds;
            }
        }
    }
}
```

```
        ignore;
    }
    odu-bdi {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-lck {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-oci {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-sd {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-tca-bbe {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-tca-es {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-tca-ses {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    odu-tca-uas {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
    }
```

```
    ignore;
}
odu-ttim {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
opu-ptim {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-ais {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-bdi {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-bdi {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-fec-deg {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-fec-deg {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
    ignore;
}
otu-fec-exe {
    hold-time {
        down milliseconds;
        up milliseconds;
    }
}
```

```
        ignore;
    }
    otu-iae {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-sd {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-tca-bbe {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-tca-es {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-tca-ses {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-tca-uas {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
    otu-ttim {
        hold-time {
            down milliseconds;
            up milliseconds;
        }
        ignore;
    }
}
tti (odu-dapi | odu-expected-receive-dapi | odu-expected-receive-sapi | odu-sapi |
    otu-dapi | otu-expected-receive-dapi | otu-expected-receive-sapi | otu-sapi);
}
passive-monitor-mode;
```



```

(per-unit-scheduler | no-per-unit-schedule);
port-mirror-instance;
ppp-options {
  chap {
    access-profile name::;
    default-chap-secret secret;
    local-name name;
    no-rfc2486;
    passive;
  }
  compression {
    acfc;
    pfc;
  }
  dynamic-profile (dynamic-profile | junos-default-profile);
  lcp-max-conf-req number;
  lcp-restart-timer milliseconds;
  loopback-clear-timer seconds;
  ncp-max-conf-req number;
  ncp-restart-timer milliseconds;
  no-termination-request;
  pap {
    access-profile name;
    default-password password;
    local-name name;
    local-password password;
    no-rfc2486;
    passive;
  }
}
promiscuous-mode;
receive-bucket {
  overflow {
    discard;
    tag;
  }
  rate number;
  threshold number;
}
redundant-pseudo-interface-options {
  redundancy-group number;
}
satop-options {
  excessive-packet-loss-rate {
    sample-period milliseconds;
    threshold percentage;
  }
  idle-pattern number;
  (jitter-buffer-auto-adjust | jitter-buffer-latency milliseconds | jitter-buffer-packets
   number;
  payload-size number;
}
speed (100m | 10m | 1g);
stacked-vlan-tagging;
switch-options {
  switch-port port-number {

```

```
(auto-negotiation | no-auto-negotiation);
cascade-port;
link-mode (full-duplex | half-duplex);
speed (100m | 10m | 1g);
vlan-id number;
}
}
t1-options {
  alarm-compliance {
    accunet-t1-5-service;
  }
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout value;
  byte-encoding (nx56 | nx64);
  fcs (16 | 32);
  framing (esf | sf);
  idle-cycle-flags (flags | ones);
  invert-data;
  line-encoding (ami | b8zs);
  loopback (local | payload | remote);
  remote-loopback-respond;
  start-end-flag (filler | shared);
  timeslots time-slot-range;
}
t3-options {
  bert-algorithm algorithm ;
  bert-error-rate rate ;
  bert-period seconds ;
  (cbit-parity | no-cbit-parity);
  compatibility-mode {
    adtran {
      subrate value;
    }
    digital-link {
      subrate value;
    }
    kentrox {
      subrate value;
    }
    larscom;
    subrate value;
  }
  verilink;
  subrate value;
}
}
fcs (16 | 32);
(feac-loop-respond | no-feac-loop-respond);
idle-cycle-flag (flags | ones);
(long-buildout | no-long-buildout);
(loop-timing | no-loop-timing);
loopback (local | payload | remote);
(no-payload-scrambler | payload-scrambler);
(no-unframed | unframed);
```

```

    start-end-flag value (filler | shared);
}
traceoptions {
    flag (all | event | ipc | media);
}
transmit-bucket {
    overflow {
        discard;
    }
    rate number;
    threshold number;
}
(traps | no-traps);
unit unit-number {
    accept-source-mac {
        mac-address mac-address;
    }
    accounting-profile name;
    arp-resp (restricted | unrestricted);
    backup-options {
        interface interface-name;
    }
    bandwidth bandwidth;
    description text;
    disable;
    encapsulation (dix | ether-vpls-fr | frame-relay-ppp | ppp-over-ether | vlan-bridge |
        vlan-ccc | vlan-vpls |vlan-tcc);
    family {
        bridge {
            bridge-domain-type (svlan| bvlan);
            filter {
                group number;
                input filter-name;
                input-list [filter-name];
                output filter-name;
                output-list [filter-name];
            }
            interface-mode (access | trunk);
            policer {
                input input-policer-name;
                output outputpolicer-name;
            }
            vlan-id vlan-id;
            vlan-id-list [vlan-id];
            vlan-rewrite {
                translate {
                    from-vlan-id;
                    to-vlan-id ;
                }
            }
        }
    }
}
ccc {
    filter {
        group number;
        input filter-name;
        input-list [filter-name];
    }
}

```

```

        output filter-name;
        output-list [filter-name];
    }
    policer {
        input input-policer-name;
        output output-policer-name;
    }
}
ethernet-switching {
    native-vlan-id native-vlan-id;
    port-mode (access | tagged-access | trunk);
    reflective-relay;
    vlan {
        members [member-name];
    }
}
inet {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
    address (source-address/prefix) {
        arp destination-address {
            (mac mac-address | multicast-mac multicast-mac-address);
            publish publish-address;
        }
        broadcast address;
        preferred;
        primary;
        vrrp-group group-id {
            (accept-data | no-accept-data);
            advertise-interval seconds;
            advertisements-threshold number;
            authentication-key key-value;
            authentication-type (md5 | simple);
            fast-interval milliseconds;
            inet6-advertise-interval milliseconds
            (preempt <hold-timesseconds> | no-preempt );
            priority value;
            track {
                interface interface-name {
                    bandwidth-threshold bandwidth;
                    priority-cost value;
                }
                priority-hold-time seconds;
                route route-address{
                    routing-instance routing-instance;
                    priority-cost value;
                }
            }
        }
        virtual-address [address];
        virtual-link-local-address address;
        vrrp-inherit-from {

```

```

        active-group value;
        active-interface interface-name;
    }
}
web-authentication {
    http;
    https;
    redirect-to-https;
}
}
dhcp {
    client-identifier {
        (ascii string | hexadecimal string);
    }
    lease-time (length | infinite);
    retransmission-attempt value;
    retransmission-interval seconds;
    server-address server-address;
    update-server;
    vendor-id vendor-id ;
}
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 ;
}
filter {
    group number;
    input filter-name;
    input-list [filter-name];
    output filter-name;
    output-list [filter-name];
}
mtu value;
no-neighbor-learn;
no-redirects;
policer {
    arp arp-name;
    input input-name;
    output output-name;
}
primary;
rpf-check {
    fail-filter filter-name;

```

```
    mode {
        loose;
    }
}
sampling {
    input;
    output;
    simple-filter;
}
targeted-broadcast {
    (forward-and-send-to-re | forward-only);
}
unnumbered-address {
    interface-name;
    preferred-source-address preferred-source-address;
}
}
inet6 {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
}
address source-address/prefix {
    eui-64;
    ndp address {
        (mac mac-address | multicast-mac multicast-mac-address);
        publish;
    }
    preferred;
    primary;
    vrrp-inet6-group group_id {
        (accept-data | no-accept-data);
        advertisements-threshold number;
        authentication-key value;
        authentication-type (md5 | simple);
        fast-interval milliseconds;
        inet6-advertise-interval milliseconds;
        (preempt <hold-time seconds> | no-preempt );
        priority value;
        track {
            interface interface-name {
                bandwidth-threshold value;
                priority-cost value;
            }
            priority-hold-time seconds;
            route route-address {
                routing-instance routing-instance;
            }
        }
    }
    virtual-inet6-address [address];
    virtual-link-local-address address;
    vrrp-inherit-from {
        active-group value;
    }
}
```

```

        active-interface interface-name;
    }
}
web-authentication {
    http;
    https;
    redirect-to-https;
}
}
(dad-disable | no-dad-disable);
dhcpv6-client {
    client-ia-type (ia-na | ia-pd);
    client-identifier duid-type (duid-ll | duid-llt | vendor);
    client-type (autoconfig | stateful);
    rapid-commit;
    req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server |
        sip-domain | sip-server | time-zone | vendor-spec);
    retransmission-attempt number;
    update-router-advertisement {
        interface interface-name;
    }
    update-server;
}
filter {
    group number;
    input filter-name;
    input-list [filter-name];
    output filter-name;
    output-list [filter-name];
}
mtu value;
nd6-stale-time seconds;
no-neighbor-learn;
policer {
    input input-name;
    output output-name;
}
rpf-check {
    fail-filter filter-name;
    mode {
        loose;
    }
}
sampling {
    input;
    output;
}
unnumbered-address {
    interface-name;
    preferred-source-address preferred-source-address;
}
}
iso {
    address source-address;
    mtu value;
}

```

```
mlfr-end-to-end {
    bundle bundle-name;
}
mlfr-uni-nni {
    bundle bundle-name;
}
mlppp {
    bundle bundle-name;
}
mpls {
    filter {
        group number;
        input filter-name;
        input-list [filter-name];
        output filter-name;
        output-list [filter-name];
    }
    mtu mtu-value;
    policer {
        input input-name;
        output output-name;
    }
}
tcc {
    policer {
        input input-name;
        output output-name;
    }
    proxy {
        inet-address inet-address;
    }
    remote {
        inet-address inet-address;
        mac-address mac-address;
    }
}
vpls {
    filter {
        group number;
        input filter-name;
        input-list [filter-name];
        output filter-name;
        output-list [filter-name];
    }
    policer {
        input input-name;
        output output-name;
    }
}
input-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | push | swap);
    tag-protocol-id tpid;
    vlan-id number;
```



```

}
interface-shared-with {
    psd-name;
}
native-inner-vlan-id value;
(no-traps | traps);
output-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | push | swap);
    tag-protocol-id tpid;
    vlan-id number;
}
ppp-options {
    chap {
        access-profile name;
        default-chap-secret name;
        local-name name;
        no-rfc2486;
        passive;
    }
    dynamic-profile profile-name;
    lcp-max-conf-req number;
    lcp-restart-timer milliseconds;
    loopback-clear-timer seconds;
    ncp-max-conf-req number;
    ncp-restart-timer milliseconds;
    no-termination-request;
    pap {
        access-profile name;
        default-password password;
        local-name name;
        local-password password;
        no-rfc2486;
        passive;
    }
}
proxy-arp (restricted | unrestricted);
radio-router {
    bandwidth number;
    credit {
        interval number;
    }
    data-rate number;
    latency number;
    quality number;
    resource number;
    threshold number;
}
swap-by-poppush;
traps;
vlan-id vlan-id;
vlan-id-range vlan-id-range;
vlan-id-list [vlan-id];
vlan-id-range vlan-id1-vlan-id2;
vlan-tags {

```

```

        (inner vlan-id | inner-range vlan-id1-vlan-id2);
        inner-list [vlan-id];
        outer vlan-id;
    }
}
vlan-tagging;
}
}

```

Related Documentation

- *Understanding Interfaces*

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

- *CLI User Guide*

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 passsword;
  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;
        propogate-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;
        }
    }
    traceoptions {
        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;
traceoptions {
  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;  
}
```

Related Documentation

- [Security Configuration Statement Hierarchy on page 57](#)

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;
}
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;  
    }  
}  
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>name</i>; primary-wins <i>name</i>; secondary-dns <i>name</i>; secondary-wins <i>name</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 706 |

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. |
| Related Documentation | <ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217• <i>Administration Guide for Security Devices</i> |

allow-configuration-regexps

| | |
|---------------------------------|--|
| Syntax | <code>allow-configuration-regexps "regular expression 1" "regular expression 2";</code> |
| Hierarchy Level | <code>[edit system login class class-name]</code> |
| 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 allow configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access.</p> <p>The statement deny-configuration-regexps takes precedence if it is 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. 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> |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 • <i>Administration Guide for Security Devices</i> |

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 1113• <i>Administration Guide for Security Devices</i> |

authentication-order

| | |
|---------------------------------|--|
| Syntax | <code>authentication-order [<i>authentication-methods</i>];</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 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 | <p><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:</p> <ul style="list-style-type: none"> • password—Use the password configured for the user with the authentication statement at the [edit system login user] hierarchy level. • radius—Use RADIUS authentication services. • tacplus—Use TACACS+ authentication services. |
| 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 the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication</i> • <i>authentication</i> |

boot-server (NTP)

| | |
|---------------------------------|--|
| Syntax | <code>boot-server (address hostname);</code> |
| Hierarchy Level | [edit system ntp] |
| 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 1113• <i>Administration Guide for Security Devices</i> |


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 1113 • <i>Administration Guide for Security Devices</i> |


broadcast-client

| | |
|---------------------------------|---|
| Syntax | <code>broadcast-client;</code> |
| Hierarchy Level | <code>[edit system ntp]</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 1113• <i>Administration Guide for Security Devices</i> |

ciphers

| | |
|--|--|
| Syntax | <code>ciphers [<i>cipher-1 cipher-2 cipher-3</i> ...]</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. • 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 | 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 217 |

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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

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 | <p>ia-na— Identity association for nontemporary address</p> <p>ia-pd—Identity association for prefix delegation</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 959 |

client-identifier (dhcp-client)

| | |
|---------------------------------|--|
| Syntax | <pre>client-identifier { user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i>; use-interface-description {logical device}; prefix [host-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] |
| 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 | <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 959 |

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 | duid-type —The DHCPv6 client is identified by a DHCP unique identifier (DUID).
duid-ll —Link Layer address.
duid-llt —Link Layer address plus time.
vendor —Vendor-assigned unique ID based on the enterprise number. |
| 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 959 |

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 | snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Understanding the SNMP Implementation in Junos OS on page 1800• Standard SNMP MIBs Supported by Junos OS on page 1804 |

client-type

| | |
|---------------------------------|---|
| Syntax | <code>client-type (autoconfig statefull);</code> |
| 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"> • <code>autoconfig</code>—Autoconfig client type for router advertisement • <code>statefull</code>—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 959 |

deny-configuration

| | |
|---------------------------------|---|
| Syntax | <code>deny-configuration "<i>regular-expression</i>";</code> |
| 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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 • <i>Administration Guide for Security Devices</i> |

deny-configuration-regexps

| | |
|---------------------------------|--|
| Syntax | <code>deny-configuration-regexps "regular expression 1" "regular expression 2";</code> |
| Hierarchy Level | <code>[edit system login class class-name]</code> |
| 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 | <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 | <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">• System Configuration Statement Hierarchy on page 217• <i>Administration Guide for Security Devices</i> |

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 920 |

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 920](#)

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 920](#)

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 920](#)

dhcpcv6 (System Services)

```
Syntax  dhcpcv6 {
        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 920 |

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 920 |

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 920 |

dlv

| | |
|---------------------------------|--|
| Syntax | dlv {
domain-name <i>domain-name</i> trusted-anchor <i>trusted-anchor</i> ;
} |
| 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 920 |

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: SRX1400, SRX3400, SRX3600, 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. |

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• <i>Junos OS System Log Reference for Security Devices</i> |
|------------------------------|---|

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: SRX1400, SRX3400, SRX3600, 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 External BGP Peering Sessions*
- *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 920• DHCP Server Configuration Overview on page 924 |
|------------------------------|--|

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 866 • Generating a Self-Signed SSL Certificate on page 866 |

hostkey-algorithm

| | |
|---------------------------------|--|
| Syntax | hostkey-algorithm <algorithm no-algorithm> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Junos OS Release 11.2.
<algorithm no algorithm> 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> NOTE: DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode.</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 866• Generating a Self-Signed SSL Certificate on page 866 |

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 920 • DHCP Server Configuration Overview on page 924 |

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">• <i>Administration Guide for Security Devices</i> |

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 | <p><i>interface-name</i> —Name of the interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p> |
| Required Privilege Level | <p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Understanding Security Zones</i> • <i>Building Blocks Feature Guide for Security Devices</i> |

interface-traceoptions (System Services DHCP)

| | |
|----------------------------|---|
| Syntax | <pre> interface-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>; 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><i>file-name</i>—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><i>files number</i>—(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><i>flag flag</i>—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 920 |
| | • DHCP Server Configuration Overview on page 924 |

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 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 217 |

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 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 217 |

lease-time (dhcp-client)

| | |
|---------------------------------|---|
| Syntax | lease-time <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 to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information. |
| Options | seconds — Request time to negotiate and exchange information. |
| 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 920 |


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 | 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 217 |

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: 120
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">• System Configuration Statement Hierarchy on page 217 |

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 217 |

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 | <p>value—Maximum number of pre-authentication SSH packets that the server will accept.</p> <p>Range: 20 through 2147483647.</p> <p>Default: 128</p> |
| 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 899 |

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 | <p>address—(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups.</p> <p>Default: 224.0.1.1.</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 1113 • <i>Administration Guide for Security Devices</i> |

name-server (Access)

| | |
|---------------------------------|--|
| Syntax | <code>name-server address;</code> |
| Hierarchy Level | [edit access address-assignment pool <i>pool-name</i> 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 1060• <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 | <pre> ntp { authentication-key <i>key-number</i> type <i>md5</i> value <<i>password</i>>; boot-server <<i>address</i>>; broadcast <<i>address</i>> <key <i>key-number</i>> <routing-instance <i>routing-instance-name</i>> <version value> <ttl <i>value</i>>; broadcast-client; multicast-client <<i>address</i>>; peer <i>address</i> <key <i>key-number</i>> <version <i>value</i>> <prefer>; server <i>address</i> <key <i>key-number</i>> <version <i>value</i>> <prefer>; source-address <i>source-address</i> <routing-instance <i>routing-instance-name</i>>; trusted-key [<i>key-numbers</i>]; }</pre> |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | <p>Configure Network Time Protocol (NTP) on the SRX Series device.</p> <p>The remaining statements are explained separately.</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"> • System Configuration Statement Hierarchy on page 217 • <i>Administration Guide for Security Devices</i> |

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 Release 10.4 of Junos OS.
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 host name 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 1146• Configuring Outbound SSH Service on page 900 |
|------------------------------|---|

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 920 |

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 1113 • <i>Administration Guide for Security Devices</i> |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

profilerd

| | |
|---------------------------------|--|
| Syntax | <pre>profilerd { 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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

protocol-version

| | |
|---------------------------------|---|
| Syntax | <code>protocol-version <i>version</i>;</code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced before Junos OS Release 11.4. |
| Description | Specify the SSH protocol versions supported. |
| Default | v2—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4. |
| Options | <i>version</i> —SSH protocol version: v1, v2, or both. |
| 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. |
| Related Documentation | <ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217 |

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 1122 |

radius-server

Syntax `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;
 }`

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 Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP).

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.

- Options**
- **server-address**—Address of the RADIUS server.
 - **accounting-port *port-number***—RADIUS server accounting port number.
Range: 1 through 65,335 files
Default: 1813
 - **port *port-number***—RADIUS server authentication port number.
Range: 1 through 65,335 files
Default: 1812
 - **retry *value***—Number of times that the router is allowed to attempt to contact a RADIUS server.
Range: 1 through 10
Default: 3
 - **secret *password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.
 - **max-outstanding-requests *value***—Maximum number of outstanding requests in flight to server.
Range: 1 through 65,335 files
 - **source-address *source-address***—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.
 - **timeout *seconds***—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.

Related Documentation • [System Configuration Statement Hierarchy on page 217](#)

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 • [Interfaces Configuration Statement Hierarchy on page 1012](#)
 • [DHCPv6 Client Overview on page 959](#)
 • [Understanding DHCPv6 Client and Server Identification on page 958](#)

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 | <ul style="list-style-type: none"> • DHCP Server, Client, and Relay Agent Overview on page 920 • DHCP Server Configuration Overview on page 924 |

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 <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 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. |
| Required Privilege Level | 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 | <ul style="list-style-type: none"> • Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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. |
| Related Documentation | <ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217 |

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. |
| Related Documentation | <ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217 |

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 1113• <i>Administration Guide for Security Devices</i> |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

services (System Services)

```
Syntax  services {
    apply-groups [ group-names ];
    apply-groups-except [ group-names ];
    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 netbios-name-server;
        }
        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 netbios-name-server;
}
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 {
    data {
        dscp (alias | bits);
        forwarding-class class-name;
    }
    dscp (alias | bits);
    forwarding-class class-name;
}
}
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 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;
  }
}
service-deployment {
  servers {
    address IPv4 address {
      security-options {
        ssl3;
        tls;
      }
      user username;
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (no-world-readable | world-readable);
    }
    flag flag ;
    no-remote-trac;
  }
  local-certificate local-certificate;
  source-address source-address;
}
}
ssh {
  connection-limit number;
  port port-number;
  rate-limit number;
}
telnet {
  connection-limit number;
  rate-limit number;
}
tftp-server {
  connection-limit number;
  rate-limit number;
}
web-management {
  http {
    interfaces interface-names ;
    port port;
  }
  https {
    interfaces interface-names;
  }
}

```

```

        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;
    }
}
xnm-clear-text {
    connection-limit number;
    rate-limit number;
}
xnm-ssl {
    connection-limit number;
    rate-limit number;
}
}

```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

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

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring the Junos OS to Work with SRC Software*

source-address (NTP, RADIUS, System Logging, or TACACS+)

| | |
|---------------------------------|--|
| Syntax | <code>source-address <i>source-address</i> <routing-instance <i>routing-instance-name</i>>;</code> |
| Hierarchy Level | [edit system accounting destination radius <i>server server-address</i>],
[edit system accounting destination tacplus <i>server server-address</i>],
[edit system <i>ntp</i>],
[edit system <i>radius-server server-address</i>],
[edit system <i>syslog</i>],
[edit system <i>tacplus-server 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 | <i>source-address</i> —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 1113 • <i>Administration Guide for Security Devices</i> |

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 1012 |

static-subscribers

| | |
|---------------------------------|--|
| Syntax | static-subscribers {
disable;
} |
| 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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

statistics-service

| | |
|---------------------------------|--|
| Syntax | statistics-service {
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 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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

subscriber-management

| | |
|---------------------------------|--|
| Syntax | <pre>subscriber-management {
 command <i>binary-file-path</i>;
 disable;
}</pre> |
| 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. |
| Related Documentation | <ul style="list-style-type: none">• System Configuration Statement Hierarchy on page 217 |

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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

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 859 |

tacplus-options

| | |
|---------------------------------|---|
| Syntax | <pre>tacplus-options { (exclude-cmd-attribute no-cmd-attribute-value); service-name <i>service-name</i>; }</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>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p>no-cmd-attribute-value and exclude-cmd-attribute options introduced in Junos OS Release 9.3.</p> <p>no-cmd-attribute-value and exclude-cmd-attribute options introduced in Junos OS Release 9.3 for EX Series switches.</p> |
| Description | Configure TACACS+ options for authentication and accounting. |
| Options | <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> |
| 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 a TACACS+ Server for System Authentication on page 859 |

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 859](#)

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 Release 10.4 of Junos OS. |
| 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 Level | trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration. |
|---------------------------------|---|

| | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Displaying Log and Trace Files on page 1485• <i>Administration Guide for Security Devices</i> |
|------------------------------|--|

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 | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

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 1113• <i>Administration Guide for Security Devices</i> |

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> • System Configuration Statement Hierarchy on page 217 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

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 | <ul style="list-style-type: none"> • Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

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 | <code>vendor-id</code> —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 | <ul style="list-style-type: none">• Interfaces Configuration Statement Hierarchy on page 1012 |

vpn (Forwarding Options)

| | |
|---------------------------------|---|
| Syntax | vpn; |
| Hierarchy Level | [edit forwarding-options helpers bootp]
[edit forwarding-options helpers bootp interface <i>interface-name</i>] |
| 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 920 |

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. |
| Related Documentation | <ul style="list-style-type: none"> • System Configuration Statement Hierarchy on page 217 |

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 | 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 217 |

web-management (System Services)

```
Syntax  web-management {
        http {
            interfaces interface-names ;
            port port;
        }
        https {
            interfaces interface-names;
            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.

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 accept 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 configuration.
- **pki-local-certificate**—X.509 certificate to use from PKI local store.
- **system-generated-certificate**—X.509 certificate generated automatically by system.

management url *management url*—URL Path for Web management access.

session—Configure web management session.

- **idle-timeout** *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 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 **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 daemon init process.
 - **mgd**—Trace MGD requests.
 - **webauth**—Trace webauth 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 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

- *WLAN Configuration Statement Hierarchy*
- *Firewall User Authentication Overview*
- *Dynamic VPN Overview*

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 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 \(Maintenance\)](#)
- [request system software abort in-service-upgrade \(ICU\)](#)
- [request system software add \(Maintenance\)](#)
- [request system software reboot](#)
- [request system software rollback \(Maintenance\)](#)
- [request support information](#)
- [request system zeroize](#)
- [restart \(Reset\)](#)
- [Restart Commands Overview on page 1229](#)
- [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 directory-usage](#)
- [show system download](#)
- [show system license \(View\)](#)

- [show system login lockout](#)
- [show system services dhcp client](#)
- [show system services dhcp relay-statistics](#)
- [show system snapshot media](#)
- [show system storage \(View SRX Series\)](#)
- [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 1234 |
| 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 1237 |
| 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 1239 |
| 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 1241 |
| 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 1243 |
| 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 1245 |
| 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 1247 |
| 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 1249 |
| Output Fields | This command produces no output. |

clear dhcpv6 server binding (Local Server)

| | |
|---------------------------------|---|
| Syntax | <pre>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>></pre> |
| 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"> • <i>all</i>—(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 1251 |

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 1255 |

clear system login logout

| | |
|---------------------------------|---|
| Syntax | clear system login logout
<all>
<username> |
| 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.

<username>—Clear the specified locked user account. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show system login logout on page 1269 |
| 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 1174
file archive (Single File) on page 1174
file archive (with Compression) on page 1174 |
| 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 1177• file checksum sha-256 on page 1178 |
| List of Sample Output | file checksum md5 on page 1176 |
| 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 1176 • file checksum sha-256 on page 1178 |
| List of Sample Output | file checksum sha1 on page 1177 |
| 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 1177• file checksum md5 on page 1176 |
| List of Sample Output | file checksum sha-256 on page 1178 |
| 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 1180</p> <p>file compare files context on page 1180</p> <p>file compare files unified on page 1180</p> <p>file compare files unified ignore-white-space on page 1180</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 1182](#)
- [Copy a Configuration File Between Routing Engines on page 1183](#)
- [Copy a Log File Between Routing Engines on page 1183](#)
- [Copy a File Using FTP on page 1183](#)
- [Copy a File Using FTP and Requiring a Password on page 1183](#)
- [Copy a File Using Secure Copy on page 1183](#)

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 1184 |
| 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 1185 |
| 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 1186 |
| 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 1187 |
| 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 1189 |
| 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 | Prepares 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 283 |
| List of Sample Output | request system autorecovery state save on page 1191
request system autorecovery state recover on page 1191
request system autorecovery state clear on page 1191 |
| 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. |
| 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 command until a Clear operation is performed. |
| <div> NOTE: Only downloads in the active, paused, and error states can be aborted.</div> | |
| Options | <code>download-id</code> —(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 266• request system download pause on page 264• request system download resume on page 265• request system download clear on page 263 |
| List of Sample Output | request system download abort on page 1192 |
| 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. |
| 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 266• request system download pause on page 264• request system download resume on page 265• request system download abort on page 262 |
| List of Sample Output | request system download clear on page 1193 |
| 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. |
| 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 266• request system download resume on page 265• request system download abort on page 262• request system download clear on page 263 |
| List of Sample Output | request system download pause on page 1194 |
| 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. |
| 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 | <p>download-id—(Required) The ID number of the download to be paused.</p> <p>max-rate—(Optional) The maximum bandwidth for the download.</p> |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • request system download start on page 266 • request system download pause on page 264 • request system download abort on page 262 • request system download clear on page 263 |
| List of Sample Output | request system download resume on page 1195 |
| 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. |
| 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 264• request system download resume on page 265• request system download abort on page 262• request system download clear on page 263 |
| List of Sample Output | request system download start on page 1196 |
| 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 90 |
| List of Sample Output | request system firmware upgrade on page 1197 |
| 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 | trial —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 115 |
| List of Sample Output | request system license update on page 1198
request system license update trial on page 1198 |
| 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"> • <i>Installation and Upgrade Guide for Security Devices</i> |
| List of Sample Output | request system halt power-off fpc on page 1199
request system power-off power-off fpc on page 1199
request system reboot power-off fpc on page 1199 |
| 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 | <code>request system services dhcp (release <i>interface-name</i> renew <i>interface-name</i>)</code> |
| 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 118 |
| List of Sample Output | request system services dhcp client release ge-1/0/1 on page 1200
request system services dhcp client renew ge-1/0/1 on page 1200 |
| Output Fields | This command produces no output. |

Sample Output

`request system services dhcp client release ge-1/0/1`

```
user@host> request system services dhcp client release ge-1/0/1
```

Sample Output

`request system services dhcp client renew ge-1/0/1`

```
user@host> request system services dhcp client renew ge-1/0/1
```

request system snapshot (Maintenance)

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**
- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
 - **media**— (Optional) Specifies the media to be included in the snapshot:
 - **compact-flash**— Copies the snapshot to an external compact flash.
 - **hard-disk**— Copies the snapshot to a hard disk.
 - **usb**— Copies the snapshot to the USB storage device.
 - **internal**— Copies the snapshot to internal media. This is the default.



NOTE: USB option is available on all SRX series devices; hard disk and compact-flash options are available only on high-end SRX series devices; media internal option is available only on branch SRX series devices.

- **node**— (Optional) Specifies to archive the data and executable areas of a specific node.
 - **node-id**—Archive a specific node. The range of node ID is (0,1)
 - **all**—Archive all nodes.
 - **local**—Archive only local nodes.
 - **primary**—Archive only 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.
- You cannot partition a hard-disk as it is mounted on /var directory.

- 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.
- The slice partition is supported only on branch SRX Series devices.

Required Privilege Level maintenance

Related Documentation [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 162](#)

List of Sample Output [request system snapshot media hard-disk on page 1202](#)
[request system snapshot media usb \(when usb device is missing on page 1202](#)
[request system snapshot media compact-flash on page 1203](#)
[request system snapshot media internal on page 1203](#)
[request system snapshot partition on page 1203](#)

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 (dals1a)...
```



```
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 media internal

```
user@host> request system snapshot media internal  
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 1204 |
| 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 | Installs 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 software reboot on page 278 |

request system software reboot

| | |
|---------------------------------|--|
| Syntax | <code>request system software reboot <at time> <in minutes><media><message 'text'></code> |
| Release Information | Command introduced in Junos OS Release 10.1. |
| Description | Reboots the software. |
| Options | <ul style="list-style-type: none">• at time— Specifies the time at which to reboot the device . You can specify time in one of the following ways:<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">• internal— Reboots from the internal media. This is the default.• usb— Reboots from the USB storage device.• external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.• message "text"— Provides a message to display to all system users before the device reboots. <p>Example: request system reboot at 5 in 50 media internal message stop</p> |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• request system software rollback (Maintenance) on page 279 |

request system software rollback (Maintenance)

| | |
|---------------------------------|--|
| Syntax | request system software rollback |
| Release Information | Command introduced in Junos OS Release 10.1. |
| Description | Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• request system software reboot on page 278 |

request support information

| | |
|---|---|
| List of Syntax | Syntax on page 1208
Syntax (SRX Series) on page 1208
Syntax (EX Series Switch and MX Series Router) on page 1208
Syntax (TX Matrix Router) on page 1208
Syntax (TX Matrix Plus Router) on page 1208 |
| Syntax | request support information |
| Syntax (SRX Series) | request support information
<node (<i>node id</i> all local primary)> |
| Syntax (EX Series Switch and MX Series Router) | request support information
<all-members>
<local>
<member <i>member-id</i> > |
| Syntax (TX Matrix Router) | request support information
<all-lcc lcc <i>number</i> scc> |
| Syntax (TX Matrix Plus Router) | request support information
<all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> > |
| Release Information | Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Display information about the system. Issue this command before contacting customer support, and then include the command output in your support request. Output from this command varies somewhat, depending on which platform you issue the command from. However, the command always executes a series of show commands, with the appropriate information for your device automatically included. |
| Options | <p>node<i>node-id</i>—(SRX Series) (Optional) Display system information for the specified node. On SRX Series, replace <i>node-id</i> with a value of 0 or 1. This option is applicable only the device with HA environment.</p> <p>all—(SRX Series) (Optional) Display system information for all nodes.</p> <p>local—(SRX Series) (Optional) Display system information for local node.</p> <p>primary—(SRX Series) (Optional) Display system information for primary node.</p> <p>all-chassis—(TX Matrix and TX Matrix Plus routers) (Optional) Display system information for all chassis.</p> <p>all-lcc—(TX Matrix and TX Matrix Plus routers) (Optional) On a TX Matrix router, display system information for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display system information for all chassis for all T1600 routers (or line-card chassis) connected to the TX Matrix Plus router.</p> |

all-members—(EX Series switches and MX Series routers) (Optional) Display system information for all members of the Virtual Chassis configuration.

lcc *number*—(TX Matrix and TX Matrix Plus routers) (Optional) On a TX Matrix router, display system information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system storage information for a specific T1600 router that is connected to the TX Matrix Plus router. Replace ***number*** with a value from 0 through 3.

local—(EX Series switches and MX Series routers) (Optional) Display system information for the local Virtual Chassis member.

member *member-id*—(EX Series switches and MX Series routers) (Optional) Display system information for the specified member of the Virtual Chassis configuration. On EX Series switches, replace ***member-id*** with a value appropriate for that Virtual Chassis configuration. On MX Series routers, replace ***member-id*** with a value of 0 or 1.

scc—(TX Matrix routers) (Optional) Display system information for the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers) (Optional) Display system information for the TX Matrix Plus router (or switch-fabric chassis). Replace ***number*** with 0.

Additional Information The **show** commands issued as a result of this command vary depending on which platform you issue the command from. Output is always appropriate for the device. For example, [Table 102 on page 1209](#) lists the **show** commands that are called when you issue **request support information** on an MX Series router.

Table 102: Sample show Commands Called by the request information support command on an MX Series Router

| | |
|---|---|
| show chassis alarms no-forwarding | show pfe statistics traffic |
| show chassis environment no-forwarding | show route summary |
| show chassis firmware no-forwarding | show system boot-messages no-forwarding |
| show chassis fpc detail | show system buffer no-forwarding |
| show chassis hardware detail no-forwarding | show system core-dumps no-forwarding |
| show chassis hardware extensive no-forwarding | show system processes extensive no-forwarding |
| show chassis routing-engine no-forwarding | show system queues no-forwarding |
| show configuration except SECRET-DATA | show system statistics no-forwarding |
| show interfaces extensive no-forwarding | show system storage no-forwarding |
| show krt queue | show system uptime no-forwarding |

Table 102: Sample show Commands Called by the request information support command on an MX Series Router (*continued*)

| | |
|---|---|
| show krt state | show system virtual-memory no-forwarding |
| show pfe statistics error | show version detail no-forwarding |
| <p>The no-forwarding option ensures that all mgd processes associated with the show command are properly halted if you break into the output (Ctrl+C) while the command is still running.</p> | |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> Request Support Information Overview |
| List of Sample Output | request support information save on page 1210
request support information scc (TX Matrix Router) on page 1210
request support information sfc (TX Matrix Plus Router) on page 1211
request support information (SRX Series) on page 1214 |
| Output Fields | For information about output fields, see the description for the specific command—listed in the output— in which you are interested. |

Sample Output

request support information | save

```
user@host> request support information | save  goose
Wrote 1143 lines of output to 'goose'
```

request support information scc (TX Matrix Router)

```
user@host> request support information scc
```

```
user@host> show system uptime
```

```
scc-re0:
```

```
-----
Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 12:53:26 PDT (11:55:40 ago)
Protocols started: 2004-09-14 12:54:19 PDT (11:54:47 ago)
Last configured: 2004-09-14 13:07:47 PDT (11:41:19 ago) by user
12:49AM PDT up 11:56, 3 users, load averages: 0.00, 0.02, 0.03
```

```
lcc0-re0:
```

```
-----
Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 15:36:41 PDT (09:12:25 ago)
Last configured: 2004-09-14 15:38:06 PDT (09:11:00 ago) by root
12:49AM PDT up 9:12, 0 users, load averages: 0.13, 0.05, 0.02
```

```
lcc2-re0:
```



```

Current time: 2004-09-15 00:49:06 PDT
System booted: 2004-09-14 15:36:47 PDT (09:12:19 ago)
Last configured: 2004-09-14 15:38:09 PDT (09:10:57 ago) by root
12:49AM PDT up 9:12, 0 users, load averages: 0.00, 0.00, 0.00

```

```
user@host> show version
```

```
scc-re0:
```

```

-----
Hostname: hostA
Model: TX Matrix
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]
JUNOS Support Tools Package [7.0-20040908.0]

```

```
lcc0-re0:
```

```

-----
Hostname: hostB
Model: t640
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]

```

```
lcc2-re0:
```

```

-----
Hostname: dewey
Model: t640
JUNOS Base OS boot [7.0I20040914_1707_mapte]
JUNOS Base OS Software Suite [7.0I20040907_1922_rtuplur]
JUNOS Kernel Software Suite [7.0I20040914_1707_mapte]
JUNOS Packet Forwarding Engine Support (T-Series) [7.0I20040914_1707_mapte]
JUNOS Routing Software Suite [7.0I20040914_1707_mapte]
JUNOS Online Documentation [7.0I20040914_1707_mapte]
JUNOS Crypto Software Suite [7.0I20040914_1707_mapte]
...

```

The output sample is truncated to display some of the support details.

request support information sfc (TX Matrix Plus Router)

```
user@host> request support information sfc 0
```

```
sfc0-re0:
```

```
user@host> show system uptime no-forwarding
```

```

Current time: 2009-05-25 03:43:28 PDT
System booted: 2009-05-25 01:15:04 PDT (02:28:24 ago)
Protocols started: 2009-05-25 01:16:01 PDT (02:27:27 ago)
Last configured: 2009-05-25 03:03:42 PDT (00:39:46 ago) by user
3:43AM up 2:28, 7 users, load averages: 0.00, 0.00, 0.00

```

```

user@host> show version detail no-forwarding

Hostname: aj
Model: txp
JUNOS Base OS boot [9.6-20090519.0]
JUNOS Base OS Software Suite [9.6-20090519.0]
JUNOS Kernel Software Suite [9.6-20090519.0]
...
user@host> show system core-dumps no-forwarding

-rw----- 1 root wheel 152223744 May 25 03:10 /var/crash/vmcore.0
-rw-r--r-- 1 bdeleon field 139417 May 22 10:17
/var/tmp/aj-core-apps-config-n-gres.txt
...
user@host> show chassis alarms no-forwarding

9 alarms currently active
Alarm time          Class  Description
2009-05-25 01:27:08 PDT  Minor  LCC 0 Minor Errors
2009-05-25 01:27:08 PDT  Minor  Spare SIB F13 6 Fault
...
user@host> show chassis hardware detail no-forwarding

Hardware inventory:
Item              Version  Part number  Serial number  Description
Chassis           REV 05   710-022574   JN112F007AHB   TXP
Midplane          REV 03   710-024027   TS4027         SFC Midplane
FPM Display       REV 03   710-024027   DX0282         TXP FPM Display
...
user@host> show system processes extensive no-forwarding

last pid: 6639; load averages: 0.00, 0.00, 0.00 up 0+02:28:54 03:43:28
161 processes: 5 running, 138 sleeping, 18 waiting

Mem: 236M Active, 227M Inact, 104M Wired, 392M Cache, 69M Buf, 2296M Free
Swap: 2048M Total, 2048M Free

  PID USERNAME   THR PRI NICE   SIZE    RES STATE    TIME    WCPU COMMAND
    11 root       1  171  52     0K     12K RUN     143:00 96.78% idle
   1530 root       1   96   0  38160K 24812K select    2:54  1.12% chassisd
   1343 root       1   76   0     0K     12K      0:18  0.00% bcmLINK.0
   1345 root       1   76   0     0K     12K      0:15  0.00% brq17: uhci1
uhci*
...
user@host> show pfe statistics error

Slot 4

SLCHIP Error statistics:

SLCHIP              0          1
-----
Lin XIF             :          0          0
Lin SRCTL            :          0          0
...
user@host> show pfe statistics traffic

Packet Forwarding Engine traffic statistics:

```

```

Input packets:          2590754          0 pps
Output packets:         2640010          0 pps
Packet Forwarding Engine local traffic statistics:
  Local packets input      :          2064527
  Local packets output     :          2115925
  Software input control plane drops :           0
  Software input high drops :           0
  Software input medium drops :           0
  Software input low drops  :           0
  Software output drops     :           0
  Hardware input drops      :           0
Packet Forwarding Engine local protocol statistics:
  HDLC keepalives          :           0
  ATM OAM                   :           0
  Frame Relay LMI           :           0
  PPP LCP/NCP               :           0
  OSPF hello                :          20048
  OSPF3 hello               :           109
  RSVP hello                :          3485
  LDP hello                 :          7191
  BFD                       :           0
  IS-IS IIH                 :          11318
  LACP                      :           0
  ARP                       :           629
  ETHER OAM                 :           930
  Unknown                   :          13212
Packet Forwarding Engine hardware discard statistics:
  Timeout                   :           0
  Truncated key             :           0
  Bits to test              :           0
  Data error                :           0
  Stack underflow           :           0
  Stack overflow            :           0
  Normal discard            :          18060
  Extended discard          :           0
  Invalid interface         :           0
  Info cell drops           :           0
  Fabric drops              :           0
Packet Forwarding Engine Input IPv4 Header Checksum Error and Output MTU Error
statistics:
  Input Checksum            :           0
  Output MTU                :           0

```

```
user@host> show chassis routing-engine no-forwarding
```

```
Routing Engine status:
```

```
Slot 0:
```

```

Current state          Master
Election priority       Master (default)
Temperature             32 degrees C / 89 degrees F
CPU temperature         46 degrees C / 114 degrees F
DRAM                   3327 MB

```

```
...
```

```
user@host> show chassis environment no-forwarding
```

```

Class Item              Status      Measurement
Temp PEM 0              OK        30 degrees C / 86 degrees F

```

```
...
```

```
user@host> show chassis firmware no-forwarding
```

```

Part                    Type          Version

```

```

Global FPC 4
Global FPC 6
Global FPC 7
...
user@host> show system boot-messages no-forwarding
...

```

The output sample is truncated to display some of the support details.

request support information (SRX Series)

```

user@host> request support information node 0
node0:
-----

user@host> show system uptime

node0:
-----
Current time: 2015-06-16 04:27:48 GMT-8
System booted: 2015-06-16 03:49:54 GMT-8 (00:37:54 ago)
Protocols started: 2015-06-16 03:52:18 GMT-8 (00:35:30 ago)
Last configured: 2015-06-16 03:50:49 GMT-8 (00:36:59 ago) by root
4:27AM up 38 mins, 1 user, load averages: 0.00, 0.02, 0.07

user@host> show version detail no-forwarding

Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.3I20150610_x_123_x48.0-718822]
JUNOS wmi Daemon [12.1I20140304_0803-tjzhang]
KERNEL 12.3I20150610_x_123_x48.0-718822 #0 built by slt-builder on 2015-06-10
13:02:52
MGD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 15:05:39 UTC
CLI release 12.3I20150610_x_123_x48.0-718822 built by slt-builder on 2015-06-10
12:30:21 UTC
RPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:41:54 UTC
CHASSISD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by
slt-builder on 2015-06-10 14:42:21 UTC
IKED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:33:31 UTC
PKID release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:19:23 UTC
SEND release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:12:44 UTC
FIPSD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:18:35 UTC
DFWD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:25:22 UTC
...
user@host> show system core-dumps no-forwarding

/var/crash/*core*: No such file or directory
-rw-rw---- 1 root wheel 966335 Jun 16 03:21 /var/tmp/nsd.core-tarball.0.tgz
-rw-rw---- 1 root wheel 940085 Jun 16 03:21 /var/tmp/nsd.core-tarball.1.tgz
-rw-rw---- 1 root wheel 963878 Jun 16 03:21 /var/tmp/nsd.core-tarball.2.tgz
-rw-rw---- 1 root wheel 940030 Jun 16 03:21 /var/tmp/nsd.core-tarball.3.tgz
-rw-rw---- 1 root wheel 1087631 Jun 16 03:22 /var/tmp/nsd.core-tarball.4.tgz

```

```

/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
total files: 5

```

```
user@host> show chassis alarms no-forwarding
```

```
No alarms currently active
```

```
user@host> show chassis hardware detail no-forwarding
```

```
Hardware inventory:
```

| Item | Version | Part number | Serial number | Description |
|----------------|----------|-----------------|------------------|-------------------------|
| Chassis | | | BH2310AA0003 | SRX1400 |
| Midplane | REV 02 | 711-031012 | AABC5474 | SRX1k Backplane |
| PEM 0 | rev 0B | 740-032015 | J027GA00030BP | AC Power Supply |
| CB 0 | Rev 03 | 750-032544 | AABL4040 | SRX1K-RE-12-10 |
| Routing Engine | | BUILTIN | BUILTIN | Routing Engine |
| ad0 | 1006 MB | CF 1GB | 2010B 0000063651 | Compact Flash |
| ad2 | 15392 MB | Wintec SSD 16GB | WT1027AA01608A9 | Hard Disk |
| CPP | | BUILTIN | BUILTIN | Central PFE Processor |
| Mezz | REV 08 | 710-021035 | AABR7876 | SRX HD Mezzanine Card |
| FPC 0 | REV 08 | 750-031019 | AABC5527 | SRX1k 10GE SYSIO |
| PIC 0 | | BUILTIN | BUILTIN | 6x 1GE RJ45 3x 1GE SFP |
| 3x 10GE SFP+ | | | | |
| FPC 1 | REV 03 | 750-032543 | AABZ2024 | SRX1k Dual Wide NPC+SPC |
| Support Card | | | | |
| PIC 0 | | BUILTIN | BUILTIN | SPU Cp-Flow |
| FPC 3 | REV 03 | 710-017865 | AABV5157 | BUILTIN NPC |
| PIC 0 | | BUILTIN | BUILTIN | NPC PIC |
| Fan Tray | -N/A- | -N/A- | -N/A- | SRX 1400 Fan Tray |

```
user@host> show system processes extensive no-forwarding
```

```

last pid: 1633; load averages: 0.00, 0.02, 0.07 up 0+00:38:27 04:27:51
261 processes: 3 running, 231 sleeping, 1 zombie, 26 waiting

```

```

Mem: 311M Active, 66M Inact, 88M Wired, 244M Cache, 110M Buf, 272M Free
Swap: 2046M Total, 2046M Free

```

| PID | USERNAME | THR | PRI | NICE | SIZE | RES | STATE | TIME | WCPU | COMMAND |
|------|----------|-----|-----|------|--------|--------|--------|-------|--------|----------|
| 11 | root | 1 | 171 | 52 | 0K | 16K | RUN | 34:19 | 81.45% | idle |
| 1600 | root | 1 | 100 | 0 | 38716K | 26760K | select | 0:00 | 13.66% | cli |
| 1601 | root | 1 | 129 | 0 | 42776K | 4260K | select | 0:00 | 4.90% | mgd |
| 60 | root | 1 | -8 | 0 | 0K | 16K | mdwait | 0:30 | 2.20% | md0 |
| 1306 | root | 1 | 98 | 0 | 122M | 16484K | select | 0:47 | 1.17% | chassisd |
| ... | | | | | | | | | | |

```
user@host> request support information node all
```

```
node0:
```

```
user@host> show system uptime
```

```
node0:
```

```
Current time: 2015-06-16 04:29:04 GMT-8
```

```

System booted: 2015-06-16 03:49:54 GMT-8 (00:39:10 ago)
Protocols started: 2015-06-16 03:52:18 GMT-8 (00:36:46 ago)
Last configured: 2015-06-16 03:50:49 GMT-8 (00:38:15 ago) by root
4:29AM up 39 mins, 1 user, load averages: 0.32, 0.14, 0.11

```

```
user@host> show version detail no-forwarding
```

```

Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.3I20150610_x_123_x48.0-718822]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.3I20150610_x_123_x48.0-718822 #0 built by slt-builder on 2015-06-10
13:02:52
MGD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 15:05:39 UTC
CLI release 12.3I20150610_x_123_x48.0-718822 built by slt-builder on 2015-06-10
12:30:21 UTC
RPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:41:54 UTC
CHASSISD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by
slt-builder on 2015-06-10 14:42:21 UTC
IKED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:33:31 UTC
PKID release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:19:23 UTC
SENDD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:12:44 UTC
FIPSD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:18:35 UTC
DFWD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:25:22 UTC
DCD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:14:34 UTC
SNMPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:58 UTC
MIB2D release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:35:05 UTC
VRRPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:22:28 UTC
...
user@host> show system core-dumps no-forwarding

```

```

/var/crash/*core*: No such file or directory
-rw-rw---- 1 root wheel 966335 Jun 16 03:21 /var/tmp/nsd.core-tarball.0.tgz
-rw-rw---- 1 root wheel 940085 Jun 16 03:21 /var/tmp/nsd.core-tarball.1.tgz
-rw-rw---- 1 root wheel 963878 Jun 16 03:21 /var/tmp/nsd.core-tarball.2.tgz
-rw-rw---- 1 root wheel 940030 Jun 16 03:21 /var/tmp/nsd.core-tarball.3.tgz
-rw-rw---- 1 root wheel 1087631 Jun 16 03:22 /var/tmp/nsd.core-tarball.4.tgz
/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
total files: 5

```

```
user@host> show chassis alarms no-forwarding
```

```
No alarms currently active
```

```
user@host> show chassis hardware detail no-forwarding
```

Hardware inventory:

| Item | Version | Part number | Serial number | Description |
|----------------|----------|-----------------|------------------|-------------------------|
| Chassis | | | BH2310AA0003 | SRX1400 |
| Midplane | REV 02 | 711-031012 | AABC5474 | SRX1k Backplane |
| PEM 0 | rev 0B | 740-032015 | J027GA00030BP | AC Power Supply |
| CB 0 | Rev 03 | 750-032544 | AABL4040 | SRX1K-RE-12-10 |
| Routing Engine | | BUILTIN | BUILTIN | Routing Engine |
| ad0 | 1006 MB | CF 1GB | 2010B 0000063651 | Compact Flash |
| ad2 | 15392 MB | Wintec SSD 16GB | WT1027AA01608A9 | Hard Disk |
| CPP | | BUILTIN | BUILTIN | Central PFE Processor |
| Mezz | REV 08 | 710-021035 | AABR7876 | SRX HD Mezzanine Card |
| FPC 0 | REV 08 | 750-031019 | AABC5527 | SRX1k 10GE SYSIO |
| PIC 0 | | BUILTIN | BUILTIN | 6x 1GE RJ45 3x 1GE SFP |
| 3x 10GE SFP+ | | | | |
| FPC 1 | REV 03 | 750-032543 | AABZ2024 | SRX1k Dual Wide NPC+SPC |
| Support Card | | | | |
| PIC 0 | | BUILTIN | BUILTIN | SPU Cp-Flow |
| FPC 3 | REV 03 | 710-017865 | AABV5157 | BUILTIN NPC |
| PIC 0 | | BUILTIN | BUILTIN | NPC PIC |
| Fan Tray | -N/A- | -N/A- | -N/A- | SRX 1400 Fan Tray |

```
user@host> show system processes extensive no-forwarding
```

```
last pid: 1865; load averages: 0.38, 0.15, 0.12 up 0+00:39:43 04:29:07
262 processes: 3 running, 231 sleeping, 1 zombie, 27 waiting
```

```
Mem: 317M Active, 66M Inact, 92M Wired, 243M Cache, 110M Buf, 263M Free
Swap: 2046M Total, 2046M Free
```

| PID | USERNAME | THR | PRI | NICE | SIZE | RES | STATE | TIME | WCPU | COMMAND |
|---------------|----------|-----|-----|------|--------|--------|--------|-------|--------|-------------|
| 11 | root | 1 | 171 | 52 | 0K | 16K | RUN | 35:12 | 78.66% | idle |
| 1832 | root | 1 | 104 | 0 | 38716K | 26876K | select | 0:00 | 14.01% | cli |
| 1833 | root | 1 | 111 | 0 | 42776K | 4264K | select | 0:00 | 4.55% | mgd |
| 1306 | root | 1 | 100 | 0 | 122M | 16556K | select | 0:49 | 1.17% | chassisd |
| 1826 | root | 1 | 96 | 0 | 42748K | 2936K | select | 0:00 | 0.35% | mgd |
| 60 | root | 1 | -8 | 0 | 0K | 16K | mdwait | 0:31 | 0.00% | md0 |
| 13 | root | 1 | -20 | -139 | 0K | 16K | WAIT | 0:13 | 0.00% | swi7: clock |
| 1326 | root | 1 | 96 | 0 | 15740K | 9396K | select | 0:05 | 0.00% | utmd |
| 1325 | root | 1 | 96 | 0 | 13108K | 7380K | select | 0:05 | 0.00% | rtlogd |
| 1360 | root | 1 | 96 | 0 | 72428K | 28828K | select | 0:04 | 0.00% | authd |
| 1329 | root | 1 | 96 | 0 | 12632K | 7672K | select | 0:04 | 0.00% | |
| license-check | | | | | | | | | | |
| 1390 | root | 1 | 96 | 0 | 33884K | 16776K | select | 0:04 | 0.00% | mib2d |
| 41 | root | 1 | 171 | 52 | 0K | 16K | pgzero | 0:04 | 0.00% | pagezero |
| 1386 | root | 1 | 96 | 0 | 30380K | 22472K | select | 0:04 | 0.00% | snmpd |
| 1379 | root | 104 | 8 | 0 | 37064K | 5576K | nanslp | 0:03 | 0.00% | wmic |
| ... | | | | | | | | | | |

```
user@host> request support information node local
node0:
```

```
user@host> show system uptime
```

```
node0:
```

```
Current time: 2015-06-16 04:31:26 GMT-8
```

```

System booted: 2015-06-16 03:49:54 GMT-8 (00:41:32 ago)
Protocols started: 2015-06-16 03:52:18 GMT-8 (00:39:08 ago)
Last configured: 2015-06-16 03:50:49 GMT-8 (00:40:37 ago) by root
4:31AM up 42 mins, 1 user, load averages: 0.29, 0.30, 0.19

```

```
user@host> show version detail no-forwarding
```

```

Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.3I20150610_x_123_x48.0-718822]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.3I20150610_x_123_x48.0-718822 #0 built by slt-builder on 2015-06-10
13:02:52
MGD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 15:05:39 UTC
CLI release 12.3I20150610_x_123_x48.0-718822 built by slt-builder on 2015-06-10
12:30:21 UTC
RPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:41:54 UTC
CHASSISD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by
slt-builder on 2015-06-10 14:42:21 UTC
IKED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:33:31 UTC
PKID release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:19:23 UTC
SENDD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:12:44 UTC
FIPSD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:18:35 UTC
DFWD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:25:22 UTC
DCD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:14:34 UTC
SNMPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:58 UTC
MIB2D release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:35:05 UTC
VRRPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:22:28 UTC
ALARMD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:12 UTC
PFED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:26:32 UTC
CRAFTD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:14 UTC
...

```

```
user@host> show system core-dumps no-forwarding
```

```

/var/crash/*core*: No such file or directory
-rw-rw---- 1 root wheel 966335 Jun 16 03:21 /var/tmp/nsd.core-tarball.0.tgz
-rw-rw---- 1 root wheel 940085 Jun 16 03:21 /var/tmp/nsd.core-tarball.1.tgz
-rw-rw---- 1 root wheel 963878 Jun 16 03:21 /var/tmp/nsd.core-tarball.2.tgz
-rw-rw---- 1 root wheel 940030 Jun 16 03:21 /var/tmp/nsd.core-tarball.3.tgz
-rw-rw---- 1 root wheel 1087631 Jun 16 03:22 /var/tmp/nsd.core-tarball.4.tgz
/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
total files: 5

```



```
user@host> show chassis alarms no-forwarding
```

```
No alarms currently active
```

```
user@host> show chassis hardware detail no-forwarding
```

```
Hardware inventory:
```

| Item | Version | Part number | Serial number | Description |
|----------------|-----------------|-------------|------------------|-------------------------|
| Chassis | | | BH2310AA0003 | SRX1400 |
| Midplane | REV 02 | 711-031012 | AABC5474 | SRX1k Backplane |
| PEM 0 | rev 0B | 740-032015 | J027GA00030BP | AC Power Supply |
| CB 0 | Rev 03 | 750-032544 | AABL4040 | SRX1K-RE-12-10 |
| Routing Engine | | BUILTIN | BUILTIN | Routing Engine |
| ad0 | 1006 MB CF 1GB | | 2010B 0000063651 | Compact Flash |
| ad2 | 15392 MB Wintec | SSD 16GB | WT1027AA01608A9 | Hard Disk |
| CPP | | BUILTIN | BUILTIN | Central PFE Processor |
| Mezz | REV 08 | 710-021035 | AABR7876 | SRX HD Mezzanine Card |
| FPC 0 | REV 08 | 750-031019 | AABC5527 | SRX1k 10GE SYSIO |
| PIC 0 | | BUILTIN | BUILTIN | 6x 1GE RJ45 3x 1GE SFP |
| 3x 10GE SFP+ | | | | |
| FPC 1 | REV 03 | 750-032543 | AABZ2024 | SRX1k Dual Wide NPC+SPC |
| Support Card | | | | |
| PIC 0 | | BUILTIN | BUILTIN | SPU Cp-Flow |
| FPC 3 | REV 03 | 710-017865 | AABV5157 | BUILTIN NPC |
| PIC 0 | | BUILTIN | BUILTIN | NPC PIC |
| Fan Tray | -N/A- | -N/A- | -N/A- | SRX 1400 Fan Tray |
| ... | | | | |

```
user@host> request support information node primary
```

```
node0:
```

```
user@host> show system uptime
```

```
node0:
```

```
-----
Current time: 2015-06-16 04:32:19 GMT-8
System booted: 2015-06-16 03:49:54 GMT-8 (00:42:25 ago)
Protocols started: 2015-06-16 03:52:18 GMT-8 (00:40:01 ago)
Last configured: 2015-06-16 03:50:49 GMT-8 (00:41:30 ago) by root
4:32AM up 42 mins, 1 user, load averages: 0.59, 0.41, 0.24
```

```
user@host> show version detail no-forwarding
```

```
Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.3I20150610_x_123_x48.0-718822]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.3I20150610_x_123_x48.0-718822 #0 built by slt-builder on 2015-06-10
13:02:52
MGD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 15:05:39 UTC
CLI release 12.3I20150610_x_123_x48.0-718822 built by slt-builder on 2015-06-10
12:30:21 UTC
RPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:41:54 UTC
CHASSISD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by
slt-builder on 2015-06-10 14:42:21 UTC
IKED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
```

```

on 2015-06-10 14:33:31 UTC
PKID release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:19:23 UTC
SENDD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:12:44 UTC
FIPSD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:18:35 UTC
DFWD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:25:22 UTC
DCD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:14:34 UTC
SNMPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:58 UTC
MIB2D release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:35:05 UTC
VRRPD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:22:28 UTC
ALARMD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:12 UTC
PFED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:26:32 UTC
CRAFTD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:21:14 UTC
SAMPLED release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:17:23 UTC
JFLOWD release 12.3I20150610_x_123_x48.0-718822 [slt-builder] built by slt-builder
on 2015-06-10 14:34:07 UTC

```

```
...
```

```
user@host> show system core-dumps no-forwarding
```

```

/var/crash/*core*: No such file or directory
-rw-rw---- 1 root wheel 966335 Jun 16 03:21 /var/tmp/nsd.core-tarball.0.tgz
-rw-rw---- 1 root wheel 940085 Jun 16 03:21 /var/tmp/nsd.core-tarball.1.tgz
-rw-rw---- 1 root wheel 963878 Jun 16 03:21 /var/tmp/nsd.core-tarball.2.tgz
-rw-rw---- 1 root wheel 940030 Jun 16 03:21 /var/tmp/nsd.core-tarball.3.tgz
-rw-rw---- 1 root wheel 1087631 Jun 16 03:22 /var/tmp/nsd.core-tarball.4.tgz
/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
total files: 5

```

```
user@host> show chassis alarms no-forwarding
```

```
No alarms currently active
```

```
user@host> show chassis hardware detail no-forwarding
```

```
Hardware inventory:
```

| Item | Version | Part number | Serial number | Description |
|----------------|----------|-----------------|------------------|-----------------------|
| Chassis | | | BH2310AA0003 | SRX1400 |
| Midplane | REV 02 | 711-031012 | AABC5474 | SRX1k Backplane |
| PEM 0 | rev 0B | 740-032015 | J027GA00030BP | AC Power Supply |
| CB 0 | Rev 03 | 750-032544 | AABL4040 | SRX1K-RE-12-10 |
| Routing Engine | | BUILTIN | BUILTIN | Routing Engine |
| ad0 | 1006 MB | CF 1GB | 2010B 0000063651 | Compact Flash |
| ad2 | 15392 MB | Wintec SSD 16GB | WT1027AA01608A9 | Hard Disk |
| CPP | | BUILTIN | BUILTIN | Central PFE Processor |
| Mezz | REV 08 | 710-021035 | AABR7876 | SRX HD Mezzanine Card |
| FPC 0 | REV 08 | 750-031019 | AABC5527 | SRX1k 10GE SYSIO |

| | | | | |
|--------------|--------|------------|----------|-------------------------|
| PIC 0 | | BUILTIN | BUILTIN | 6x 1GE RJ45 3x 1GE SFP |
| 3x 10GE SFP+ | | | | |
| FPC 1 | REV 03 | 750-032543 | AABZ2024 | SRX1k Dual Wide NPC+SPC |
| Support Card | | | | |
| PIC 0 | | BUILTIN | BUILTIN | SPU Cp-Flow |
| FPC 3 | REV 03 | 710-017865 | AABV5157 | BUILTIN NPC |
| PIC 0 | | BUILTIN | BUILTIN | NPC PIC |
| Fan Tray | -N/A- | -N/A- | -N/A- | SRX 1400 Fan Tray |

```
user@host> show system processes extensive no-forwarding
```

```
last pid: 2336; load averages: 0.70, 0.44, 0.25 up 0+00:42:58 04:32:22
267 processes: 2 running, 236 sleeping, 2 zombie, 27 waiting
```

```
Mem: 321M Active, 66M Inact, 92M Wired, 243M Cache, 110M Buf, 258M Free
Swap: 2046M Total, 2046M Free
```

| PID | USERNAME | THR | PRI | NICE | SIZE | RES | STATE | TIME | WCPU | COMMAND |
|------|----------|-----|-----|------|--------|--------|--------|-------|--------|----------|
| 11 | root | 1 | 171 | 52 | 0K | 16K | RUN | 37:36 | 68.12% | idle |
| 2303 | root | 1 | 107 | 0 | 38716K | 26876K | select | 0:00 | 14.01% | cli |
| 2304 | root | 1 | 119 | 0 | 42776K | 4264K | select | 0:00 | 5.60% | mgd |
| 2295 | root | 1 | -8 | 0 | 2352K | 1120K | pipe | 0:00 | 3.39% | awk |
| 2294 | root | 1 | 102 | 0 | 2508K | 1352K | select | 0:00 | 2.07% | cprod |
| 1306 | root | 1 | 100 | 0 | 122M | 16556K | select | 0:53 | 1.17% | chassisd |
| 2068 | root | 1 | -8 | 0 | 42748K | 2936K | pipe | 0:01 | 0.78% | mgd |
| 2296 | root | 1 | -8 | 0 | 3936K | 2692K | pipe | 0:00 | 0.75% | less |
| 2297 | root | 1 | 97 | 0 | 42748K | 2936K | select | 0:00 | 0.70% | mgd |
| 41 | root | 1 | 171 | 52 | 0K | 16K | pgzero | 0:05 | 0.39% | pagezero |
| 1593 | root | 1 | 98 | 0 | 42812K | 3348K | select | 0:05 | 0.10% | mgd |
| 1587 | root | 1 | 97 | 0 | 7964K | 3088K | select | 0:00 | 0.10% | ssh |
| ... | | | | | | | | | | |

The output sample is truncated to display some of the support details.

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 software reboot on page 278](#)
- [request system software rollback \(Maintenance\) on page 279](#)

List of Sample Output [request system zeroize on page 1222](#)

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.config
/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 Initialization
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 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.
...
output truncated
```

restart (Reset)

| | |
|-------------------------------------|---|
| List of Syntax | Syntax (High-end SRX Series) on page 1224
Syntax (Branch SRX Series) on page 1224 |
| Syntax (High-end SRX Series) | <pre>restart <application-identification application-security audit-process 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 fipsd firewall firewall-authentication-service general-authentication-service gprs-process gracefully idp-policy immediately interface-control ipmi ipsec-key-management jflow-service jnx-wmi-service 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 routing sampling secure-neighbor-discovery security-intelligence security-log service-deployment simple-mail-client-service soft snmp statistics-service subscriber-management subscriber-management-helper system-log-vital tunnel-oamd uac-service user-ad-authentication vrrp web-management></pre> |
| Syntax (Branch SRX Series) | <pre>restart <802.1x-protocol-daemon application-identification application-security audit-process autoinstallation chassis-control class-of-service database-replication ddns dhcp dhcp-service dialer-services dynamic-flow-capture event-processing ethernet-connectivity-fault-management ethernet-link-fault-management ethernet-switching firewall firewall-authentication-service forwarding general-authentication-service gracefully group-key-member group-key-server idp-policy immediately interface-control ipmi ipsec-key-management jnx-wmicd-service jsrp-service kernel-replication l2-learning lacp license-service lldpd-service mib-process mountd-service mpls-traceroute multicast-snooping named-service network-security network-security-trace nfsd-service ntpd-service peer-selection-service pgm profilerd pki-service ppp pppoe r2cp remote-operations routing sampling sdk-service secure-neighbor-discovery security-intelligence security-log services service-deployment simple-mail-client-service soft snmp statistics-service subscriber-management subscriber-management-helper system-health-management system-log-vital uac-service user-ad-authentication usb-control vrrp web-management wireless-lan-service wireless-wan-service></pre> |
| Release Information | <p>Command introduced before Junos OS Release 7.4.</p> <p>dynamic-flow-capture option added in Junos OS Release 7.4.</p> <p>event-processing option added in Junos OS Release 7.5.</p> <p>group-key-server option added in Junos OS Release 10.2.</p> <p>ppp option added in Junos OS Release 7.5.</p> |
| 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**
- **802.1x-protocol-daemon**—(Branch SRX Series only) (Optional) Restart the 802.1x protocol process (daemon).
 - **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.
 - **autoinstallation**—(Branch SRX Series only) (Optional) Restart the autoinstallation process.
 - **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.
 - **database-replication**—(Optional) Restart the database replication process.
 - **datapath-trace-service**—(High-end SRX Series only) (Optional) 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.
 - **dialer-services**—(Branch SRX Series only) (Optional) Restart the ISDN dial-out process.
 - **disk-monitoring**—(High-end SRX Series only) (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.
 - **ethernet-switching**—(Branch SRX Series only) (Optional) Restart the Ethernet switching process.
 - **event-processing**—(Optional) Restart the event process (eventd).
 - **fipsd**—(High-end SRX Series only) (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.
- **forwarding**—(Branch SRX Series only) (Optional) Restart the security forwarding options process.
- **general-authentication-service**—(Optional) Restart the general authentication process.
- **gprs-process**—(High-end SRX Series only) (Optional) Restart the General Packet Radio Service (GPRS) process.
- **gracefully**—(Optional) Restart the software process.
- **group-key-member**—(Branch SRX Series only) (Optional) Restart the group key member process.
- **group-key-server**—(Branch SRX Series only) (Optional) Restart the group VPN server process. The group VPN server loses all its data, including TEK and KEK keys, when it restarts. New keys are generated, but the keys are not available to group members until they reregister.
- **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**—(High-end SRX Series only) (Optional) Restart jflow service process.
- **jnx-wmi-service**—(High-end SRX Series only) (Optional) Restart the jnx Windows Management Instrumentation (WMI) service 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.
- `lldpd-service`—(Branch SRX Series only) (Optional) Restart the Link Layer Discovery Protocol (LLDP) process.
- `logical-system-service`—(High-end SRX Series only) (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.
- `mpls-traceroute`—(Branch SRX Series only) (Optional) Restart the MPLS periodic traceroute process.
- `multicast-snooping`—(Branch SRX Series only) (Optional) Restart the multicast snooping process, which makes L2 devices, such as VLAN switches, aware of L3 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-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.
- `peer-selection-service`—(Branch SRX Series only) (Optional) Restart the peer selection service 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`—(High-end SRX Series only) (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.
- `ppp`—(Branch SRX Series only) (Optional) Restart the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.
- `pppoe`—(Branch SRX Series only) (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.

- `profilerd`—(Optional) Restart the profiler process.
- `r2cp`—(Branch SRX Series only) (Optional) Restart the Radio-to-Router Control Protocol process.
- `remote-operations`—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
- `routing`—(Optional) Restart the routing protocol process (`rp`d).
- `sampling`—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.
- `sdk-service`—(Branch SRX Series only) (Optional) Restart the software development kit (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`—(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`—(Branch SRX Series only) (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.
- `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-health-management`—(Branch SRX Series only) (Optional) Restart the system health management process.
- `system-log-vital`—(Optional) Restart system log vital process.
- `tunnel-oamd`—(High-end SRX Series only) (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
- **usb-control**—(SRX branch devices only) (Optional) Restart the USB control process.
- **vrp**—(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.
- **wireless-lan-service**—(Branch SRX Series only) (Optional) Restart the wireless LAN service process.
- **wireless-wan-service**—(Branch SRX Series only) (Optional) Restart the wireless WAN service process.

Required Privilege Level reset

Related Documentation • [Restart Commands Overview on page 1229](#)

List of Sample Output [restart interfaces on page 1229](#)

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 • *CLI User Guide*

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 1562 • request system snapshot (Maintenance) on page 273 |
| List of Sample Output | show chassis routing-engine (Sample 1 - SRX240) on page 1231
show chassis routing-engine (Sample 2 - SRX650) on page 1231
show chassis routing-engine (Sample 3 - vSRX) on page 1232 |
| Output Fields | Table 103 on page 1230 lists the output fields for the show chassis routing-engine command. Output fields are listed in the approximate order in which they appear. |

Table 103: 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 103: 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 - SRX240)

```

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-SRX240-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 - SRX650)

```

user@host> show chassis routing-engine
Routing Engine status:
  Temperature           46 degrees C / 114 degrees F
  CPU temperature       46 degrees C / 114 degrees F
  Total memory          1024 MB Max  737 MB used ( 72 percent)
    Control plane memory 600 MB Max  426 MB used ( 71 percent)
    Data plane memory   424 MB Max  314 MB used ( 74 percent)
  CPU utilization:
    User                 40 percent
    Background           0 percent
    Kernel              11 percent
    Interrupt            0 percent
    Idle                 49 percent
  Model                 RE-SRXSME-SRE6
  Start time            2009-09-19 20:04:18 PDT
  Uptime                1 day, 4 hours, 51 minutes, 11 seconds
  Last reboot reason    0x200:chassis control reset

```

| | | | |
|----------------|----------|----------|-----------|
| Load averages: | 1 minute | 5 minute | 15 minute |
| | 0.27 | 0.53 | 0.78 |

Sample Output

show chassis routing-engine (Sample 3 - 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 1163 |
| List of Sample Output | show dhcp client binding on page 1235 |
| Output Fields | Table 104 on page 1234 lists the output fields for the show dhcp client binding command. Output fields are listed in the approximate order in which they appear. |

Table 104: 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 104: 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, 2.2.2.2, 3.3.3.3 ]
Name: server-identifier, Value: 10.1.1.1
Name: router, Value: [ 10.1.1.80 ]
Name: domain-name, Value: netscreen-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 <routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Display Dynamic Host Configuration Protocol (DHCP) client statistics. |
| Options | routing-instance routing-instance-name —(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 1164 |
| List of Sample Output | show dhcp client statistics on page 1238 |
| Output Fields | Table 105 on page 1237 lists the output fields for the show dhcp client statistics command. Output fields are listed in the approximate order in which they appear. |

Table 105: 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 105: 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 1165 |
| List of Sample Output | show dhcp relay binding on page 1240 |
| Output Fields | Table 106 on page 1239 lists the output fields for the show dhcp relay binding command. Output fields are listed in the approximate order in which they appear. |

Table 106: 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 106: 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 1166 |
| List of Sample Output | show dhcp relay statistics on page 1241 |
| Output Fields | Table 107 on page 1241 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear. |

Table 107: 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 1167 |
| List of Sample Output | show dhcp server binding on page 1244 |
| Output Fields | Table 108 on page 1243 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear. |

Table 108: 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 108: 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 1168 |
| List of Sample Output | show dhcp server statistics on page 1246 |
| Output Fields | Table 109 on page 1245 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear. |

Table 109: 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 1169 |
| List of Sample Output | show dhcpv6 client binding on page 1248 |
| Output Fields | Table 110 on page 1247 lists the output fields for the show dhcpv6 client binding command. Output fields are listed in the approximate order in which they appear. |

Table 110: 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 110: 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
2000::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:          2000::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 1170 |
| List of Sample Output | show dhcpv6 client statistics on page 1250 |
| Output Fields | Table 111 on page 1249 lists the output fields for the show dhcpv6 client statistics command. Output fields are listed in the approximate order in which they appear. |

Table 111: 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 | Number of DHCPv6 messages sent. <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 111: 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 1171 |
| List of Sample Output | show dhcpv6 server binding on page 1252
show dhcpv6 server binding detail on page 1253
show dhcpv6 server binding interface on page 1253
show dhcpv6 server binding interface detail on page 1253
show dhcpv6 server binding prefix on page 1254
show dhcpv6 server binding session-id on page 1254
show dhcpv6 server binding summary on page 1254 |
| Output Fields | Table 112 on page 1251 lists the output fields for the show dhcpv6 server binding command. Output fields are listed in the approximate order in which they appear. |

Table 112: show dhcvc6p 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 112: 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 1172 |
| List of Sample Output | show dhcpv6 server statistics on page 1257 |
| Output Fields | Table 113 on page 1256 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear. |

Table 113: 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 743 |
| List of Sample Output | show firewall on page 1259 |
| Output Fields | Table 114 on page 1258 lists the output fields for the show firewall command. Output fields are listed in the approximate order in which they appear. |

Table 114: 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 114: show firewall Output Fields (*continued*)

| Field Name | Field Description |
|-----------------|--|
| Counters | <p>Display filter counter information:</p> <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 | <p>Display policer information:</p> <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 | Performs checks and shows status of all autorecovered items. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • request system autorecovery state on page 260 • Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices on page 184 |
| List of Sample Output | show system autorecovery state on page 1260 |
| Output Fields | Table 33 on page 283 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear. |

Table 115: 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 directory-usage

Syntax show system directory-usage
 <depth *number*>
 <node *node-id* | all | local | primary>
 <path>

Release Information Command introduced before Junos OS Release 9.0.

Description Display directory usage information.

- Options**
- **none**—Display all directory usage information.
 - **depth *number***—(Optional) Specify the depth of the directory to traverse. This option is useful when you want to limit the output shown for a large file system.
 - **node**—(Optional) Display the directory information for a specific node.



NOTE: The **node** option is supported only on high-end SRX Series devices.

- **node-id**—Identification number of the node. It can be 0 or 1.
- **all**—(Optional) Display the directory information for all nodes.
- **local**—(Optional) Display the directory information for the local node.
- **primary**—(Optional) Display the directory information for the primary node.
- **path**—(Optional) Specify the path of the root directory to traverse.

Required Privilege Level view

Related Documentation

- *Administration Guide for Security Devices*

List of Sample Output [show system directory-usage on page 1263](#)

Output Fields [Table 116 on page 1262](#) describes the output fields for the **show system directory-usage** command. Output fields are listed in the approximate order in which they appear.

Table 116: show system directory-usage Output Fields

| Field Name | Field Description |
|-----------------------|---|
| <i>bytes</i> | Number of bytes used by files in a directory. |
| <i>directory-name</i> | Name of the directory. |

Sample Output

show system directory-usage

```
user@host> show system directory-usage
node0:
```

```
-----
          /var/tmp
2.0K      /var/tmp/.ssh
```

show system download

| | |
|---------------------------------|---|
| Syntax | <code>show system download <download-id></code> |
| Release Information | Command introduced in Junos OS Release 11.2. |
| 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 266 Understanding Download Manager for SRX Series Devices on page 135 |
| List of Sample Output | show system download on page 1264
show system download 1 on page 1265 |
| Output Fields | Table 34 on page 285 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear. |

Table 117: 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 location of the downloaded file. |

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"> • Working with License Keys for SRX Series Devices on page 209 |
| List of Sample Output | <p>show system license on page 1267</p> <p>show system license installed on page 1267</p> <p>show system license keys on page 1268</p> <p>show system license usage on page 1268</p> <p>show system license status logical-system all on page 1268</p> |
| Output Fields | Table 18 on page 115 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear. |

Table 118: 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 118: 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 user names locked after unsuccessful login attempts. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none"> • show system snapshot media on page 290 |
| List of Sample Output | show system login logout on page 1269 |
| Output Fields | <p>Table 119 on page 1269 lists the output fields for the show system login logout 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.</p> |

Table 119: 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. |
| 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"> • dhcp (Interfaces) • request system services dhcp on page 1200 |
| List of Sample Output | show system services dhcp client on page 1271
show system services dhcp client ge-0/0/1.0 on page 1271
show system services dhcp client statistics on page 1272 |
| Output Fields | Table 19 on page 118 lists the output fields for the show system services dhcp client command. Output fields are listed in the approximate order in which they appear. |

Table 120: 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 at | Date and time the lease expires. |
| DHCP Options | <ul style="list-style-type: none"> • Name: <code>server-identifier</code>, Value: IP address of the name server. • Name: <code>device</code>, Value: IP address of the name device. • Name: <code>domain-name</code>, Value: Name of the domain. |

Table 120: show system services dhcp client Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|---|
| 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-0/0/1.0
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
update server            enabled
Lease Obtained at        2006-08-24 18:13:04 PST
Lease Expires at         2006-08-25 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: domain-name, Value: netscreen-50

```

Sample Output

show system services dhcp client ge-0/0/1.0

```

user@host> show system services dhcp client ge-0/0/1.0

```

```
Logical Interface name      ge-0/0/1.0
Hardware address           00:12:1e:a9:7b:81
Client status              bound
Address obtained           30.1.1.20
Update server              disabled
Lease obtained at         2007-05-10 18:16:18 UTC
Lease expires at          2007-05-11 18:16:18 UTC
DHCP options:
  Name: server-identifier, Value: 30.1.1.2
  Code: 1, Type: ip-address, Value: 255.255.255.0
  Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
  Name: domain-name, Value: mylab.example.net
```

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 | show system services dhcp relay-statistics |
| 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 1273 |
| Output Fields | Table 121 on page 1273 lists the output fields for the show system services dhcp relay-statistics command. Output fields are listed in the approximate order in which they appear. |

Table 121: 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 compact flash. This option is available on the SRX650 Services Gateway. |
| 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 181 |

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/da1s1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/da1s2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```

show system storage (View SRX Series)

Syntax show system storage
 <detail>
 <node *node-id* | all | local | primary>
 <partitions>

Release Information Command introduced in Junos OS Release 10.2.

Description Display the local storage data currently available on the SRX Series devices.

- Options**
- **none**—Display standard information about the amount of free disk space in the device file system.
 - **detail**—(Optional) Display detailed output about the amount of free disk space in the device file system.
 - **node**—(Optional) Display local storage data for a specific node.



NOTE: The **node** option is supported only on high-end SRX Series devices.

- **node-id**—Identification number of the node. It can be 0 or 1.
- **all**—(Optional) Display the local storage data for all nodes.
- **local**—(Optional) Display the local storage data for the local node.
- **primary**—(Optional) Display the local storage data for the primary node.
- **partitions**—(Optional) Display partitions information for the boot media.



NOTE: The **partitions** option is supported only on branch SRX Series devices.

Required Privilege Level View

Output Fields [Table 36 on page 291](#) describes the output fields for the **show system storage** command. Output fields are listed in the approximate order in which they appear.

Table 122: show system storage Output Fields

| Field Name | Field Description |
|-------------------|--|
| Filesystem | Name of the file system. |
| Size | Size of the file system. |
| Used | Amount of space used in the file system. |

Table 122: show system storage Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|---|
| Avail | Amount of space available in the file system. |
| Capacity | Percentage of the file system space that is being used. |
| Mounted on | Directory in which the file system is mounted. |

show system storage

```
user@host>show system storage
```

| Filesystem | Size | Used | Avail | Capacity | Mounted on |
|--------------|------|------|-------|----------|--------------------|
| /dev/ad0s2a | 621M | 169M | 402M | 30% | / |
| devfs | 1.0K | 1.0K | 0B | 100% | /dev |
| /dev/md0 | 20M | 6.3M | 12M | 35% | /junos |
| /cf/packages | 621M | 169M | 402M | 30% | /junos/cf/packages |
| devfs | 1.0K | 1.0K | 0B | 100% | /junos/cf/dev |
| /dev/md1 | 494M | 494M | 0B | 100% | /junos |
| /cf | 20M | 6.3M | 12M | 35% | /junos/cf |
| devfs | 1.0K | 1.0K | 0B | 100% | /junos/dev/ |
| /cf/packages | 621M | 169M | 402M | 30% | /junos/cf/packages |
| 1 | | | | | |
| procfs | 4.0K | 4.0K | 0B | 100% | /proc |
| /dev/bo0s3e | 49M | 24K | 45M | 0% | /config |
| /dev/bo0s3f | 616M | 399M | 168M | 70% | /cf/var |
| /dev/md2 | 336M | 20M | 289M | 7% | /mfs |
| /cf/var/jail | 616M | 399M | 168M | 70% | /jail/var |
| /cf/var/log | 616M | 399M | 168M | 70% | /jail/var/log |
| devfs | 1.0K | 1.0K | 0B | 100% | /jail/dev |
| /dev/md3 | 63M | 4.0K | 58M | 0% | /mfs/var/run/utm |
| /dev/md4 | 1.8M | 228K | 1.5M | 13% | /jail/mfs |

show system storage partitions (View SRX Series)

| | |
|---------------------------------|---|
| Syntax | show system storage partitions |
| Release Information | Command introduced in Junos OS Release 10.2 . |
| Description | Displays 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 162 |

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
```


PART 6

Monitoring and Troubleshooting Library for Security Devices

- [Network Monitoring and Troubleshooting Guide for Security Devices on page 1283](#)
- [System Log Monitoring and Troubleshooting Guide for Security Devices on page 1717](#)
- [SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices on page 1797](#)

CHAPTER 34

Network Monitoring and Troubleshooting Guide for Security Devices

- [Overview on page 1283](#)
- [Configuring Monitoring Options on page 1310](#)
- [Monitoring Common Security Features on page 1357](#)
- [Troubleshooting on page 1477](#)
- [Configuration Statements and Operational Commands on page 1547](#)

Overview

- [Introduction to Network Monitoring on page 1283](#)
- [Accounting Options, Source Class Usage, and Destination Class Usage Overview on page 1287](#)
- [Gathering Statistics for Accounting Purposes on page 1289](#)

Introduction to Network Monitoring

- [Monitoring Overview on page 1283](#)
- [Diagnostic Tools Overview on page 1284](#)

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 1400](#)
- [Diagnostic Tools Overview on page 1284](#)

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 1285](#)
- [CLI Diagnostic Commands on page 1285](#)

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 123 on page 1285](#) describes the functions of the Troubleshoot options.

Table 123: J-Web Interface Troubleshoot Options

| Option | Function |
|-----------------------------|--|
| Troubleshoot Options | |
| 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 124 on page 1286](#).

Table 124: 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. |
| 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 1492](#)

- [Configuring Ping MPLS on page 1494](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- [Using the ping Command on page 1494](#)

Accounting Options, Source Class Usage, and Destination Class Usage Overview

- [Accounting Options Overview on page 1287](#)
- [Understanding Source Class Usage and Destination Class Usage Options on page 1288](#)

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 125 on page 1287](#).

Table 125: 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](#)
- [Accounting Options Configuration on page 1289](#)
- [Configuring Accounting-Data Log Files on page 1292](#)
- [Configuring the Interface Profile on page 1295](#)
- [Configuring the Filter Profile on page 1297](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level](#)

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.

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. On a T4000 Type 5 FPC, the source class accounting is performed at egress. The implications of this are as follows:

- SCU accounting is *not* 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).

Related Documentation

- [Configuring SCU or DCU on page 1301](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the MIB Profile on page 1307](#)
- [Configuring the Routing Engine Profile on page 1308](#)

Gathering Statistics for Accounting Purposes

- [Accounting Options Configuration on page 1289](#)
- [Configuring Accounting-Data Log Files on page 1292](#)
- [Configuring the Interface Profile on page 1295](#)
- [Configuring the Filter Profile on page 1297](#)
- [Example: Configuring a Filter Profile on page 1299](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1300](#)
- [Configuring SCU or DCU on page 1301](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the MIB Profile on page 1307](#)
- [Configuring the Routing Engine Profile on page 1308](#)

Accounting Options Configuration

This topic contains the following sections:

- [Accounting Options—Full Configuration on page 1289](#)
- [Minimum Accounting Options Configuration on page 1290](#)

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.

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 1287](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Configuring Accounting-Data Log Files on page 1292](#)
- [Configuring the Interface Profile on page 1295](#)
- [Configuring the Filter Profile on page 1297](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level](#)

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 1293](#)
- [Configuring the Maximum Size of the File on page 1293](#)
- [Configuring the Maximum Number of Files on page 1293](#)
- [Configuring the Start Time for File Transfer on page 1293](#)
- [Configuring the Transfer Interval of the File on page 1294](#)
- [Configuring Archive Sites on page 1294](#)

Configuring the Storage Location of the File

```
[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, there is a possibility of losing data 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. 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 1287](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Accounting Options Configuration on page 1289](#)

- [Configuring the Interface Profile on page 1295](#)
- [Configuring the Filter Profile on page 1297](#)
- *Configuration Statements at the [edit accounting-options] Hierarchy Level*

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.

To configure an interface profile, perform the tasks described in the following sections:

- [Configuring Fields on page 1295](#)
- [Configuring the File Information on page 1296](#)
- [Configuring the Interval on page 1296](#)
- [Example: Configuring the Interface Profile on page 1296](#)

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 1287](#)
- *Understanding Device Management Functions in Junos OS*
- [Accounting Options Configuration on page 1289](#)
- [Configuring Accounting-Data Log Files on page 1292](#)
- [Configuring the Filter Profile on page 1297](#)
- *Configuration Statements at the [edit accounting-options] Hierarchy Level*

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 1298](#)
- [Configuring the File Information on page 1298](#)
- [Configuring the Interval on page 1298](#)

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: 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 1287](#)
- [Configuring Accounting-Data Log Files on page 1292](#)
- [Example: Configuring a Filter Profile on page 1299](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1300](#)

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 1297](#)
 - [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1300](#)

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 1297](#)
- [Configuring the Interface Profile on page 1295](#)

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 1301](#)
- [Applying the Policy to the Forwarding Table on page 1302](#)
- [Enabling Accounting on Inbound and Outbound Interfaces on page 1302](#)

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 192.168.1.0/24 orlonger;
  }
  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;
          }
        }
      }
    }
  }
}
```

```

    }
  }
}

```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1288](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the MIB Profile on page 1307](#)
- [Configuring the Routing Engine Profile on page 1308](#)

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 1303](#)
- [Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface on page 1303](#)
- [Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface on page 1304](#)

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 10.255.14.225:100;
  }
}

```

```

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;
        }
      }
    }
  }
}

```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1288](#)
- [Configuring SCU or DCU on page 1301](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the MIB Profile on page 1307](#)
- [Configuring the Routing Engine Profile on page 1308](#)

Configuring Class Usage Profiles

To collect class usage statistics, perform the tasks described in these sections:

- [Configuring a Class Usage Profile on page 1305](#)
- [Configuring the File Information on page 1305](#)
- [Configuring the Interval on page 1305](#)

- [Creating a Class Usage Profile to Collect Source Class Usage Statistics on page 1305](#)
- [Creating a Class Usage Profile to Collect Destination Class Usage Statistics on page 1306](#)

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-profile;
  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 1288](#)
- [Configuring SCU or DCU on page 1301](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring the Routing Engine Profile on page 1308](#)

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 1307](#)
- [Configuring the Interval on page 1307](#)
- [Configuring the MIB Operation on page 1308](#)
- [Configuring MIB Object Names on page 1308](#)
- [Example: Configuring a MIB Profile on page 1308](#)

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.

Example: Configuring a MIB Profile

Configure a MIB profile:

```
[edit accounting-options]  
  mib-profile mstatistics {  
    file stats;  
    interval 60;  
    operation walk;  
    objects-names {  
      ipCidrRouteStatus;  
      ifOutOctets;  
    }  
  }
```

Related Documentation

- [Understanding Source Class Usage and Destination Class Usage Options on page 1288](#)
- [Configuring SCU or DCU on page 1301](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the Routing Engine Profile on page 1308](#)

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 1309](#)
- [Configuring the File Information on page 1309](#)
- [Configuring the Interval on page 1309](#)
- [Example: Configuring a Routing Engine Profile on page 1309](#)

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 1288](#)
- [Configuring SCU or DCU on page 1301](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1303](#)
- [Configuring Class Usage Profiles on page 1304](#)
- [Configuring the MIB Profile on page 1307](#)

Configuring Monitoring Options

- [Configuring Interface Alarms on page 1310](#)
- [Using RPM to Measure Network Performance on page 1321](#)
- [Configuring IP Monitoring on page 1344](#)

Configuring Interface Alarms

- [Alarm Overview on page 1310](#)
- [Example: Configuring Interface Alarms on page 1316](#)
- [Monitoring Active Alarms on a Device on page 1318](#)
- [Monitoring Alarms on page 1319](#)

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 1311](#)
- [Alarm Severity on page 1311](#)
- [Alarm Conditions on page 1311](#)

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.

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 1312](#)
- [System Alarm Conditions on page 1315](#)

Interface Alarm Conditions

Table 126 on page 1312 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 126: 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 126: 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 126: 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 126: 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 127 on page 1315](#) lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 127: System Alarm Conditions and Corrective Actions

| Alarm Type | Alarm Condition | Corrective Action |
|---------------|--------------------------------------|-------------------------------|
| Configuration | The rescue configuration is not set. | Set the rescue configuration. |

Table 127: 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 1316](#)
 - [Monitoring Active Alarms on a Device on page 1318](#)
 - [Monitoring Alarms on page 1319](#)
 - [System Log Messages](#)

Example: Configuring Interface Alarms

This example shows how to configure interface alarms.

- [Requirements on page 1316](#)
- [Overview on page 1316](#)
- [Configuration on page 1317](#)
- [Verification on page 1318](#)

Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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 1310](#).

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 into 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1310](#)
- [Monitoring Active Alarms on a Device on page 1318](#)
- [Monitoring Alarms on page 1319](#)

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 1310](#)
 - [Example: Configuring Interface Alarms on page 1316](#)
 - [Monitoring Alarms on page 1319](#)

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 128 on page 1320](#) summarizes key output fields in the alarms page.

Table 128: 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 1318](#)
- [Monitoring Events on page 1447](#)

- [Monitoring Security Events by Policy on page 1430](#)

Using RPM to Measure Network Performance

- [RPM Overview on page 1321](#)
- [RPM Support for VPN Routing and Forwarding on page 1325](#)
- [Example: Configuring Basic RPM Probes on page 1325](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1329](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1332](#)
- [Directing RPM Probes to Select BGP Devices on page 1334](#)
- [Configuring RPM Timestamping on page 1335](#)
- [Tuning RPM Probes on page 1336](#)
- [RPM Configuration Options on page 1337](#)
- [Monitoring RPM Probes on page 1340](#)

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 1321](#)
- [RPM Tests on page 1322](#)
- [Probe and Test Intervals on page 1322](#)
- [Jitter Measurement with Hardware Timestamping on page 1322](#)
- [RPM Statistics on page 1323](#)
- [RPM Thresholds and Traps on page 1324](#)
- [RPM for BGP Monitoring on page 1324](#)

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 SRX240 Low Memory devices and SRX240 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 129 on page 1323](#).

Table 129: 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 |
| 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 |

Table 129: RPM Statistics (*continued*)

| RPM Statistics | Description |
|---------------------------------|--|
| 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 1337](#)
 - [RPM Support for VPN Routing and Forwarding on page 1325](#)
 - [Example: Configuring Basic RPM Probes on page 1325](#)
 - [Monitoring RPM Probes on page 1340](#)
 - [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1536](#)

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 IP 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 1321](#)
 - [RPM Configuration Options on page 1337](#)
 - [Monitoring RPM Probes on page 1340](#)

Example: Configuring Basic RPM Probes

This example shows how to configure basic RPM probes to measure performance between two network endpoints.

- [Requirements on page 1325](#)
- [Overview on page 1326](#)
- [Configuration on page 1326](#)
- [Verification on page 1328](#)

Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 192.178.16.5;
 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 1328](#)
- [Verifying RPM Statistics on page 1328](#)

### **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 1321](#)
  - [RPM Configuration Options on page 1337](#)
  - [Tuning RPM Probes on page 1336](#)

### Example: Configuring RPM Using TCP and UDP Probes

This example shows how to configure RPM using TCP and UDP probes.

- [Requirements on page 1329](#)
- [Overview on page 1329](#)
- [Configuration on page 1330](#)
- [Verification on page 1331](#)

#### Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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 1325](#).

#### 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
{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*.

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 1321](#)
- [RPM Configuration Options on page 1337](#)
- [Example: Configuring Basic RPM Probes on page 1325](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1332](#)
- [Tuning RPM Probes on page 1336](#)

---

**Example: Configuring RPM Probes for BGP Monitoring**

---

This example shows how to configure RPM probes to monitor BGP neighbors.

- [Requirements on page 1332](#)
- [Overview on page 1332](#)
- [Configuration on page 1333](#)
- [Verification on page 1334](#)

**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 1325](#).
- 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 1329](#).

**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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1321](#)
  - [RPM Configuration Options on page 1337](#)
  - [Directing RPM Probes to Select BGP Devices on page 1334](#)
  - [Tuning RPM Probes on page 1336](#)

---

### **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*.

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 1321](#)
- [RPM Configuration Options on page 1337](#)
- [Example: Configuring Basic RPM Probes on page 1325](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1332](#)
- [Tuning RPM Probes on page 1336](#)

### Configuring RPM Timestamping

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You can timestamp the following RPM probe types: **icmp-ping**, **icmp-ping-timestamp**, **udp-ping**, and **udp-ping-timestamp**.

This example shows how to enable timestamping for customerA. The test for customerA is identified as customerA-test.

To configure timestamping:

1. Specify the RPM probe owner for which you want to enable timestamping.

```
[edit services rpm]
user@host# edit probe customerA
```

2. Specify a name for the test.

```
[edit services rpm probe customerA]
user@host# edit test customerA-test
```

3. Enable timestamping.

```
[edit services rpm probe customerA test customerA-test]
user@host# edit hardware-timestamp
```

4. (Optional) If preferred, indicate that you want timestamping to be only one-way.

```
[edit services rpm probe customerA test customerA-test]
user@host# edit one-way-hardware-timestamp
```



**NOTE:** You cannot include both the **source-address** and **hardware-timestamp** or **one-way-hardware-timestamp** statements at the **[edit services rpm probe probe-name test test-name]** hierarchy level simultaneously.

#### Related Documentation

- [RPM Overview on page 1321](#)
- [RPM Configuration Options on page 1337](#)
- [Example: Configuring Basic RPM Probes on page 1325](#)

- [Example: Configuring RPM Using TCP and UDP Probes on page 1329](#)
- [Tuning RPM Probes on page 1336](#)

### **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 1325.

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*.

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 1321](#)
- [RPM Configuration Options on page 1337](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1332](#)
- [Configuring RPM Timestamping on page 1335](#)

## RPM Configuration Options

You can configure real-time performance monitoring (RPM) parameters. See [Table 130 on page 1337](#) for a summary of the configuration options.

**Table 130: 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)	IP address or URL of probe target	Type the IP address, in dotted decimal notation, 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 IP address to be used as the probe source address	Type the source address to be used for the probe. If the source IP 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> 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>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).

Table 130: RPM Configuration Summary (*continued*)

Field	Function	Your Action
Probe Count	Sets the total number of probes to be sent for each test.	Type a number between 1 and 15.
Destination Port	Specifies the TCP or UDP port to which probes are sent.  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.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is <b>000000</b> .	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	Enables timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter: <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).



Table 130: RPM Configuration Summary (*continued*)

Field	Function	Your Action
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).
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>

Table 130: RPM Configuration Summary (*continued*)

Field	Function	Your Action
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>
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 1321](#)
- [Example: Configuring Basic RPM Probes on page 1325](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1329](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1332](#)

### 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

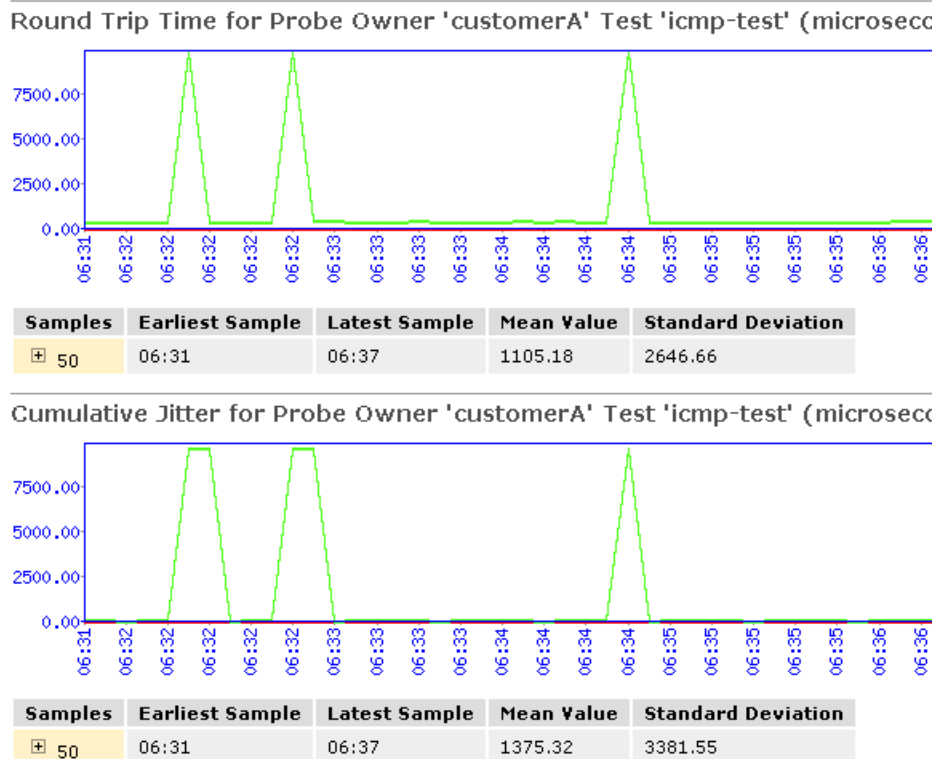
**Troubleshoot>RPM>View RPM** in the J-Web user interface, or in configuration mode enter the **show** command:

[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 45 on page 640](#) shows sample graphs for an RPM test.

**Figure 57: Sample RPM Graphs**



In [Figure 45 on page 640](#), 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 131 on page 1341](#) summarizes key output fields in RPM displays.

**Table 131: Summary of Key RPM Output Fields**

Field	Values	Additional Information
<b>Currently Running Tests</b>		
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.	—

Table 131: Summary of Key RPM Output Fields (*continued*)

Field	Values	Additional Information
Test Name	Configured name of the RPM test.	—
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>icmp-ping-timestamp</b></li> <li>• <b>tcp-ping</b></li> <li>• <b>udp-ping</b></li> </ul>	—
Target Address	IP address or URL of the remote server that is being probed by the RPM test.	—
Source Address	Explicitly configured 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.	—

Table 131: Summary of Key RPM Output Fields (*continued*)

Field	Values	Additional Information
Latest Sample	System time when the last probe in the sample was received.	–
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.	–

Table 131: Summary of Key RPM Output Fields (*continued*)

Field	Values	Additional Information
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	—

- Related Documentation**
- [RPM Overview on page 1321](#)
  - [RPM Support for VPN Routing and Forwarding on page 1325](#)
  - [RPM Configuration Options on page 1337](#)

## Configuring IP Monitoring

- [IP Monitoring Overview on page 1344](#)
- [Understanding IP Monitoring Test Parameters on page 1345](#)
- [Example: Configuring IP Monitoring on Branch SRX Series Devices on page 1346](#)
- [Understanding IP Monitoring Through Redundant Ethernet Interface Link Aggregation Groups on page 1348](#)
- [Example: Configuring IP Monitoring on High-End SRX Series Devices on page 1349](#)
- [Example: Configuring Chassis Cluster Redundancy Group IP Address Monitoring on page 1354](#)

### 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 1345](#)

### 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 132 on page 1345](#) lists the test parameters and its default values:

**Table 132: Test Parameters and Default Values**

Parameter	Default Value
probe-count	1
probe-interval	3 seconds
test-interval	1 second

[Table 133 on page 1346](#) lists the supported threshold and its description:

Table 133: 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 1344](#)

#### Example: Configuring IP Monitoring on Branch SRX Series Devices

This example shows how to monitor IP on branch SRX Series devices.

- [Requirements on page 1346](#)
- [Overview on page 1346](#)
- [Configuration on page 1346](#)
- [Verification on page 1348](#)

#### 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, past them into a text file, remove any line breaks, change any details to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1344](#)
  - [Understanding IP Monitoring Test Parameters on page 1345](#)

### **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 1344](#)

### 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 1349](#)
- [Overview on page 1349](#)
- [Configuration on page 1350](#)
- [Verification on page 1352](#)

#### **Requirements**

- You need two SRX5800 Services Gateways with identical hardware configurations, one SRX Series device (SRX650 in this example), 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.

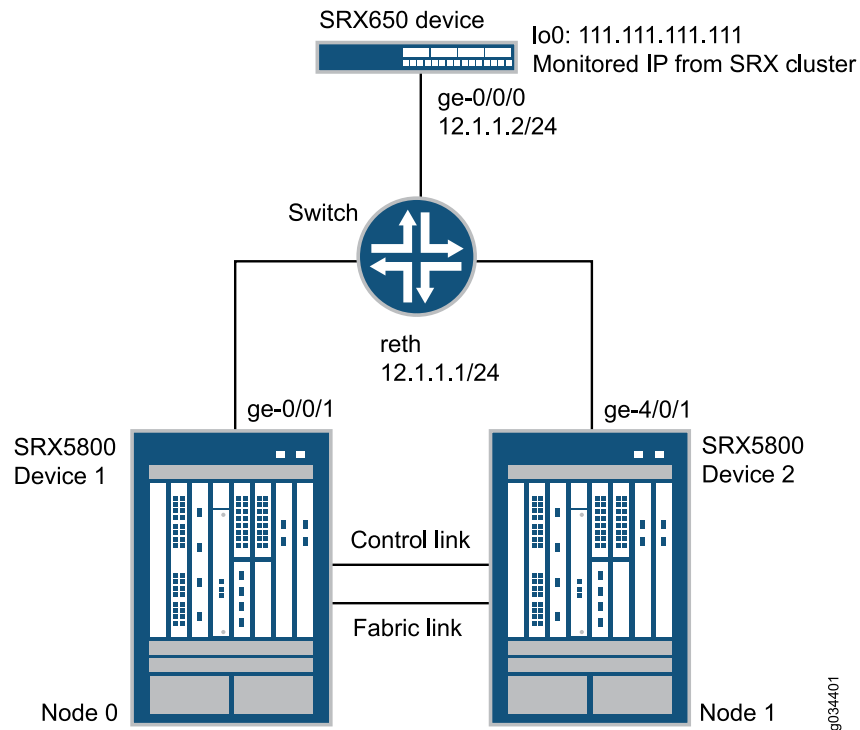


NOTE: IP monitoring is not supported on an NP-IOC card.

#### **Topology**

[Figure 58 on page 1350](#) shows the topology used in this example.

**Figure 58: 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 1351](#)

**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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1352](#)
- [Verifying Chassis Cluster IP Monitoring Status—Before Failover on page 1353](#)
- [Verifying Chassis Cluster Status—After Failover on page 1353](#)
- [Verifying Chassis Cluster IP Monitoring Status—After Failover on page 1354](#)

**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 SRX Series Services Gateway for the High-End as a Chassis Cluster*

#### **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 chassis cluster.

- [Requirements on page 1355](#)
- [Overview on page 1355](#)
- [Configuration on page 1355](#)
- [Verification on page 1357](#)



### Requirements

Before you begin:

- Set the chassis cluster node ID and cluster ID. See *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*.

### 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 redundancy group IP address monitoring, copy the following commands and paste them into the CLI:

```
{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.

For brevity, this **show** command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```

{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 0: Routing Engines](#)
  - [Understanding Chassis Cluster Redundancy Groups 1 Through 128](#)
  - [Understanding Chassis Cluster Redundancy Group Interface Monitoring](#)
  - [Understanding Chassis Cluster Redundancy Group IP Address Monitoring](#)
  - [Understanding Chassis Cluster Redundancy Group Failover](#)
  - [Understanding Chassis Cluster Monitoring of Global-Level Objects](#)

## Monitoring Common Security Features

- [Displaying Real-Time Information from Device to Host on page 1358](#)
- [Monitoring Application Layer Gateways Features on page 1362](#)
- [Monitoring Class-of-Service on page 1387](#)
- [Monitoring Interfaces and Switching Functions on page 1394](#)
- [Monitoring NAT on page 1411](#)

- [Monitoring Security Policies on page 1422](#)
- [Monitoring Events, Services and System on page 1447](#)
- [Monitoring Unified Threat Management Features on page 1455](#)
- [Monitoring VPNs on page 1466](#)

## Displaying Real-Time Information from Device to Host

- [Displaying Multicast Path Information on page 1358](#)
- [Displaying Real-Time Monitoring Information on page 1360](#)

### 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> <ttl number> <wait-time seconds> <loop>
<multicast-response | unicast-response> <no-resolve> <no-router-alert> <brief |
detail>
```

[Table 134 on page 1358](#) describes the **mtrace from-source** command options.

**Table 134: 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 0.0.0.0.
<b>interval seconds</b>	(Optional) Sets the interval between statistics gathering. The default value is 10.
<b>max-hops number</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 number</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 host</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 routing-instance-name</b>	(Optional) Traces the routing instance you specify.
<b>ttl number</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 <i>all routers</i> multicast group is 1. Otherwise, the default value is 127.
<b>wait-time seconds</b>	(Optional) Sets the time to wait for a response packet. The default value is 3 seconds.

Table 134: CLI mtrace from-source Command Options (*continued*)

Option	Description
<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 135 on page 1359 summarizes the output fields of the display.



**NOTE:** The packet statistics gathered from Juniper Networks devices and routing nodes always display as 0.

Table 135: CLI mtrace from-source Command Output Summary

Field	Description
<b>hop-number</b>	Number of the hop (device) along the path.
<b>host</b>	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.

Table 135: CLI mtrace from-source Command Output Summary (*continued*)

Field	Description
<i>ip-address</i>	IP address of the device.
<i>protocol</i>	Protocol used.
<i>tth</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 1283](#)

#### 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 136 on page 1360](#) describes the **traceroute monitor** command options.

Table 136: 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.

Table 136: CLI traceroute monitor Command Options (*continued*)

Option	Description
<b>inet6</b>	(Optional) Forces the traceroute packets to an IPv6 destination.
<b>interval seconds</b>	(Optional) Sets the interval between ping requests, in seconds. The default value is 1 second.
<b>no-resolve</b>	(Optional) Suppresses the display of the hostnames of the hops along the path.
<b>size bytes</b>	(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.
<b>source address</b>	(Optional) Uses the source address that you specify, in the traceroute packet.
<b>summary</b>	(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
9.4 8.6 4.8 9.9 2.1
2. 173.24.232.66
7.9 17.2 7.9 29.4 11.0
3. 173.24.232.66
9.9 9.3 8.7 9.9 0.5
4. 173.24.232.66
9.9 9.8 9.5 10.0 0.2

 Packets
Loss% Snt
0.0% 5
0.0% 5
0.0% 5
0.0% 5

```

[Table 137 on page 1361](#) summarizes the output fields of the display.

Table 137: 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>psize</b> <i>size</i>	Size of ping request packet, in bytes.
<b>Keys</b>	
<b>Help</b>	Displays the Help for the CLI commands.  Press H to display the Help.

Table 137: CLI traceroute monitor Command Output Summary (*continued*)

Field	Description
Display mode	Toggles the display mode. Press D to toggle the display mode
Restart statistics	Restarts the <b>traceroute monitor</b> command. Press R to restart the <b>traceroute monitor</b> command.
Order of fields	Sets the order of the displayed fields. Press O to set the order of the displayed fields.
quit	Quits the <b>traceroute monitor</b> command. Press Q to quit the <b>traceroute monitor</b> command.
Packets	
number	Number of the hop (device) along the route to the final destination host.
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 1485](#)

## Monitoring Application Layer Gateways Features

- [Monitoring H.323 ALG Information on page 1363](#)
- [Monitoring MGCP ALGs on page 1364](#)
- [Monitoring SCCP ALGs on page 1367](#)
- [Monitoring SIP ALGs on page 1369](#)



- [Monitoring Voice ALG H.323 on page 1373](#)
- [Monitoring Voice ALG MGCP on page 1375](#)
- [Monitoring Voice ALG SCCP on page 1378](#)
- [Monitoring Voice ALG SIP on page 1381](#)
- [Monitoring Voice ALG Summary on page 1386](#)

### 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 138 on page 1363](#) summarizes key output fields in the H.323 counters display.

**Table 138: 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.	—
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.	—

Table 138: Summary of Key H.323 Counters Output Fields (*continued*)

Field	Values	Additional Information
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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### Monitoring MGCP ALGs

This section contains the following topics:

- [Monitoring MGCP ALG Calls on page 1364](#)
- [Monitoring MGCP ALG Counters on page 1365](#)
- [Monitoring MGCP ALG Endpoints on page 1366](#)

#### 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 139 on page 1364](#) summarizes key output fields in the MGCP calls display.

Table 139: 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.	—

Table 139: Summary of Key MGCP Calls Output Fields (*continued*)

Field	Values	Additional Information
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 140 on page 1365](#) summarizes key output fields in the MGCP counters display.

Table 140: 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.	—
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.	—

Table 140: Summary of Key MGCP Counters Output Fields (*continued*)

Field	Values	Additional Information
<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 141 on page 1366](#) summarizes key output fields in the MGCP endpoints display.

Table 141: 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>		

Table 141: Summary of Key MGCP Endpoints Output Fields (*continued*)

Field	Values	Additional Information
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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### Monitoring SCCP ALGs

This section contains the following topics:

- [Monitoring SCCP ALG Calls on page 1367](#)
- [Monitoring SCCP ALG Counters on page 1368](#)

#### 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 142 on page 1367](#) summarizes key output fields in the SCCP calls display.

Table 142: 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 143 on page 1368](#) summarizes key output fields in the SCCP counters display.

**Table 143: 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.	—
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).	—

Table 143: Summary of Key SCCP Counters Output Fields (*continued*)

Field	Values	Additional Information
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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### Monitoring SIP ALGs

This section contains the following topics:

- [Monitoring SIP ALG Calls on page 1369](#)
- [Monitoring SIP ALG Counters on page 1370](#)
- [Monitoring SIP ALG Rate Information on page 1372](#)
- [Monitoring SIP ALG Transactions on page 1373](#)

#### 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 144 on page 1370](#) summarizes key output fields in the SIP calls display.

Table 144: 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 145 on page 1370](#) summarizes key output fields in the SIP counters display.

Table 145: 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.
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.



Table 145: Summary of Key SIP Counters Output Fields (*continued*)

Field	Values	Additional Information
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.	—
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.	—

Table 145: Summary of Key SIP Counters Output Fields (*continued*)

Field	Values	Additional Information
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 146 on page 1372](#) summarizes key output fields in the SIP rate display.

Table 146: Summary of Key SIP Rate Output Fields

Field	Values	Additional Information
<b>SIP Rate Information</b>		
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.	—

Table 146: Summary of Key SIP Rate Output Fields (*continued*)

Field	Values	Additional Information
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 147 on page 1373](#) summarizes key output fields in the SIP transactions display.

Table 147: 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 1283](#)
- [Monitoring Interfaces on page 1400](#)

**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 148 on page 1374](#) summarizes key output fields in the ALG H.323 page.

Table 148: 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

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.	—

#### Counter Summary Chart

Table 148: ALG H.323 Monitoring Page (*continued*)

Field	Value	Additional Information
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 1386](#)
  - [Monitoring Voice ALG MGCP on page 1375](#)
  - [Monitoring Voice ALG SCCP on page 1378](#)
  - [Monitoring Voice ALG SIP on page 1381](#)

### 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 149 on page 1376 summarizes key output fields in the voice ALG MGCP page.

**Table 149: 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.

#### Counters

##### MGCP Counters Summary

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.	—

Table 149: Voice ALG MGCP Monitoring Page (*continued*)

Field	Value	Additional Information
<b>MGCP Error Counter</b>		
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.	—

Table 149: Voice ALG MGCP Monitoring Page (*continued*)

Field	Value	Additional Information
<b>Calls</b>		
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 1386](#)
  - [Monitoring Voice ALG H.323 on page 1373](#)
  - [Monitoring Voice ALG SCCP on page 1378](#)
  - [Monitoring Voice ALG SIP on page 1381](#)

### 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 150 on page 1378](#) summarizes key output fields in the voice ALG SCCP page.

Table 150: 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 150: 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 150: 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 error.</li> <li>• <b>Invalid NAT cookies deleted</b>— Number of invalid NAT cookie deleted.</li> <li>• <b>NAT cookies not found</b>— Number of NAT cookie 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 1386](#)

- [Monitoring Voice ALG H.323 on page 1373](#)
- [Monitoring Voice ALG MGCP on page 1375](#)
- [Monitoring Voice ALG SIP on page 1381](#)

### 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 151 on page 1381](#) summarizes key output fields in the voice ALG SIP page.

**Table 151: 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 151: 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 151: 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 151: 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 151: 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 1386](#)
  - [Monitoring Voice ALG H.323 on page 1373](#)
  - [Monitoring Voice ALG MGCP on page 1375](#)
  - [Monitoring Voice ALG SCCP on page 1378](#)

### 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 152 on page 1386](#) summarizes key output fields in the voice ALG summary page.

**Table 152: 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 1373](#)
  - [Monitoring Voice ALG MGCP on page 1375](#)
  - [Monitoring Voice ALG SCCP on page 1378](#)
  - [Monitoring Voice ALG SIP on page 1381](#)

## Monitoring Class-of-Service

- [Monitoring Class-of-Service Performance on page 1387](#)
- [Monitoring CoS Classifiers on page 1393](#)

### Monitoring Class-of-Service Performance

The J-Web user interface provides information about the class-of-service (CoS) performance on a device. You can view information about the current status of CoS components—classifiers, CoS value aliases, red drop profiles, forwarding classes, rewrite rules and scheduler maps. You can also see the interfaces to which these components are assigned.

In addition, you can display the entire CoS configuration, including system-chosen defaults, by entering the **show class-of-service** command.

This section contains the following topics:

- [Monitoring CoS Interfaces on page 1387](#)
- [Monitoring CoS Classifiers on page 1388](#)
- [Monitoring CoS Value Aliases on page 1389](#)
- [Monitoring CoS RED Drop Profiles on page 1390](#)
- [Monitoring CoS Forwarding Classes on page 1390](#)
- [Monitoring CoS Rewrite Rules on page 1391](#)
- [Monitoring CoS Scheduler Maps on page 1392](#)

#### **Monitoring CoS Interfaces**

**Purpose** Display details about the physical and logical interfaces and the CoS components assigned to them.

**Action** Select **Monitor>Class of Service>Interfaces** in the J-Web user interface, or enter the **show class-of-service interface *interface*** command.

[Table 153 on page 1387](#) summarizes key output fields for CoS interfaces.

**Table 153: Summary of Key CoS Interfaces Output Fields**

Field	Values	Additional Information
Interface	Name of a physical interface to which CoS components are assigned.	To display names of logical interfaces configured on this physical interface, click the plus sign (+).

Table 153: Summary of Key CoS Interfaces Output Fields (*continued*)

Field	Values	Additional Information
Scheduler Map	Name of the scheduler map associated with this interface.	–
Queues Supported	Number of queues you can configure on the interface.	–
Queues in Use	Number of queues currently configured.	–
Logical Interface	Name of a logical interface on the physical interface, to which CoS components are assigned.	–
Object	Category of an object—for example, <b>classifier</b> , <b>scheduler-map</b> , or <b>rewrite</b> .	–
Name	Name that you have given to an object—for example, <b>ba-classifier</b> .	–
Type	Type of an object—for example, <b>dscp</b> , or <b>exp</b> for a classifier.	–
Index	Index of this interface or the internal index of a specific object.	–

**Monitoring CoS Classifiers**

**Purpose** Display the mapping of incoming CoS value to forwarding class and loss priority.

**Action** For each classifier, select **Monitor>Class of Service>Classifiers** in the J-Web user interface, or enter the **show class-of-service classifier** command.

[Table 154 on page 1388](#) summarizes key output fields for CoS classifiers.

Table 154: Summary of Key CoS Classifier Output Fields

Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).
CoS Value Type	The classifiers are displayed by type: <ul style="list-style-type: none"> <li>• <b>dscp</b>—All classifiers of the DSCP type.</li> <li>• <b>dscp ipv6</b>—All classifiers of the DSCP IPv6 type.</li> <li>• <b>exp</b>—All classifiers of the MPLS EXP type.</li> <li>• <b>ieee-802.1</b>—All classifiers of the IEEE 802.1 type.</li> <li>• <b>inet-precedence</b>—All classifiers of the IP precedence type.</li> </ul>	

Table 154: Summary of Key CoS Classifier Output Fields (*continued*)

Index	Internal index of the classifier.
Incoming CoS Value	CoS value of the incoming packets, in bits. These values are used for classification.
Assign to Forwarding Class	Forwarding class that the classifier assigns to an incoming packet. This class affects the forwarding and scheduling policies that are applied to the packet as it transits the device.
Assign to Loss Priority	Loss priority value that the classifier assigns to the incoming packet based on its CoS value.

**Monitoring CoS Value Aliases**

**Purpose** Display information about the CoS value aliases that the system is currently using to represent DSCP, DSCP IPv6, MPLS EXP, and IPv4 precedence bits.

**Action** Select **Monitor>Class of Service>CoS Value Aliases** in the J-Web user interface, or enter the **show class-of-service code-point-aliases** command.

[Table 155 on page 1389](#) summarizes key output fields for CoS value aliases.

Table 155: Summary of Key CoS Value Alias Output Fields

Field	Values	Additional Information
CoS Value Type	Type of the CoS value: <ul style="list-style-type: none"> <li><b>dscp</b>—Examines Layer 3 packet headers for IP packet classification.</li> <li><b>dscp ipv6</b>—Examines Layer 3 packet headers for IPv6 packet classification.</li> <li><b>exp</b>—Examines Layer 2 packet headers for MPLS packet classification.</li> <li><b>ieee-802.1</b>—Examines Layer 2 packet header for packet classification.</li> <li><b>inet-precedence</b>—Examines Layer 3 packet headers for IP packet classification.</li> </ul>	To display aliases and bit patterns, click the plus sign (+).
CoS Value Alias	Name given to a set of bits—for example, <b>af11</b> is a name for <b>001010</b> bits.	—
Bit Pattern	Set of bits associated with an alias.	—

**Monitoring CoS RED Drop Profiles**

**Purpose** Display data point information for each CoS random early detection (RED) drop profile currently on a system.

**Action** Select **Monitor>Class of Service>RED Drop Profiles** in the J-Web user interface, or enter the **show class-of-service drop-profile** command.

Table 156 on page 1390 summarizes key output fields for CoS RED drop profiles.

**Table 156: Summary of Key CoS RED Drop Profile Output Fields**

Field	Values	Additional Information
RED Drop Profile Name	Name of the RED drop profile.  A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and one for drop probability, that determine the relationship between a buffer's fullness and the likelihood it will drop packets.	To display profile values, click the plus sign (+).
Graph RED Profile	Link to a graph of a RED curve that the system uses to determine the drop probability based on queue buffer fullness.	The x axis represents the queue buffer fill level, and the y axis represents the drop probability.
Type	Type of a specific drop profile: <ul style="list-style-type: none"> <li><b>interpolated</b>—The two coordinates (x and y) of the graph are interpolated to produce a smooth profile.</li> <li><b>segmented</b>—The two coordinates (x and y) of the graph are represented by line fragments to produce a segmented profile.</li> </ul>	—
Index	Internal index of this drop profile.	—
Fill Level	Percentage fullness of a buffer queue. This value is the x coordinate of the RED drop profile graph.	—
Drop Probability	Drop probability of a packet corresponding to a specific queue buffer fill level. This value is the y coordinate of the RED drop profile graph.	—

**Monitoring CoS Forwarding Classes**

**Purpose** View the current assignment of CoS forwarding classes to queue numbers on the system.

**Action** Select **Monitor>Class of Service>Forwarding Classes** in the J-Web user interface, or enter the **show class-of-service forwarding-class** command.

Table 157 on page 1391 summarizes key output fields for CoS forwarding classes.

**Table 157: Summary of Key CoS Forwarding Class Output Fields**

Field	Values	Additional Information
Forwarding Class	Names of forwarding classes assigned to queue numbers. By default, the following forwarding classes are assigned to queues 0 through 3: <ul style="list-style-type: none"> <li>• <b>best-effort</b>—Provides no special CoS handling of packets. Loss priority is typically not carried in a CoS value, and RED drop profiles are more aggressive.</li> <li>• <b>expedited-forwarding</b>—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service.</li> <li>• <b>assured-forwarding</b>—Provides high assurance for packets within specified service profile. Excess packets are dropped.</li> <li>• <b>network-control</b>—Packets can be delayed but not dropped.</li> </ul>	—
Queue	Queue number corresponding to the forwarding class name.	By default, four queues, 0 through 3, are assigned to forwarding classes.

#### **Monitoring CoS Rewrite Rules**

**Purpose** Display information about CoS value rewrite rules, which are based on the forwarding class and loss priority.

**Action** Select **Monitor>Class of Service>Rewrite Rules** in the J-Web user interface, or enter the **show class-of-service rewrite-rules** command.

Table 158 on page 1391 summarizes key output fields for CoS rewrite rules.

**Table 158: Summary of Key CoS Rewrite Rules Output Fields**

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	—
CoS Value Type	Rewrite rule type: <ul style="list-style-type: none"> <li>• <b>dscp</b>—For IPv4 DiffServ traffic.</li> <li>• <b>dscp-ipv6</b>—For IPv6 DiffServ traffic.</li> <li>• <b>exp</b>—For MPLS traffic.</li> <li>• <b>ieee-802.1</b>—For Layer 2 traffic.</li> <li>• <b>inet-precedence</b>—For IPv4 traffic.</li> </ul>	To display forwarding classes, loss priorities, and rewritten CoS values, click the plus sign (+).
Index	Internal index for this particular rewrite rule.	—

Table 158: Summary of Key CoS Rewrite Rules Output Fields (*continued*)

Field	Values	Additional Information
Forwarding Class	Forwarding class that in combination with loss priority is used to determine CoS values for rewriting.	Rewrite rules are applied to CoS values in outgoing packets based on forwarding class and loss priority setting.
Loss Priority	Loss priority that in combination with forwarding class is used to determine CoS values for rewriting.	—
Rewrite CoS Value To	Value that the CoS value is rewritten to.	—

**Monitoring CoS Scheduler Maps**

**Purpose** Display assignments of CoS forwarding classes to schedulers.

**Action** Select **Monitor>Class of Service>Scheduler Maps** in the J-Web user interface, or enter the **show class-of-service scheduler-map** command.

Table 159 on page 1392 summarizes key output fields for CoS scheduler maps.

Table 159: Summary of Key CoS Scheduler Maps Output Fields

Field	Values	Additional Information
Scheduler Map	Name of a scheduler map.	For details, click the plus sign (+).
Index	Index of a specific object—scheduler maps, schedulers, or drop profiles.	—
Scheduler Name	Name of a scheduler.	—
Forwarding Class	Forwarding classes this scheduler is assigned to.	—
Transmit Rate	Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following: <ul style="list-style-type: none"> <li>A percentage—The scheduler receives the specified percentage of the total interface bandwidth.</li> <li><b>remainder</b>—The scheduler receives the remaining bandwidth of the interface after allocation to other schedulers.</li> </ul>	—
Rate Limit	Rate limiting configuration of the queue: <ul style="list-style-type: none"> <li><b>none</b>—No rate limiting.</li> <li><b>exact</b>—The queue transmits at only the configured rate.</li> </ul>	—

Table 159: Summary of Key CoS Scheduler Maps Output Fields (*continued*)

Field	Values	Additional Information
Buffer Size	Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following: <ul style="list-style-type: none"> <li>• A percentage—The buffer is a percentage of the total buffer allocation.</li> <li>• <b>remainder</b>—The buffer is sized according to what remains after other scheduler buffer allocations.</li> </ul>	—
Priority	Scheduling priority of a queue: <ul style="list-style-type: none"> <li>• <b>high</b>—Packets in this queue are transmitted first.</li> <li>• <b>low</b>—Packets in this queue are transmitted last.</li> <li>• <b>medium-high</b>—Packets in this queue are transmitted after high-priority packets.</li> <li>• <b>medium-low</b>—Packets in this queue are transmitted before low-priority packets.</li> </ul>	—
Drop Profiles	Name and index of a drop profile that is assigned to a specific loss priority and protocol pair.	—
Loss Priority	Packet loss priority corresponding to a drop profile: <ul style="list-style-type: none"> <li>• <b>low</b>—Packet has a low loss priority.</li> <li>• <b>high</b>—Packet has a high loss priority.</li> <li>• <b>medium-low</b>—Packet has a medium-low loss priority.</li> <li>• <b>medium-high</b>—Packet has a medium-high loss priority.</li> </ul>	—
Protocol	Transport protocol corresponding to a drop profile.	—
Drop Profile Name	Name of the drop profile.	—

- Related Documentation**
- [Monitoring Overview on page 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### Monitoring CoS Classifiers

**Purpose** Display the mapping of incoming CoS value to forwarding class and loss priority.

**Action** For each classifier, select **Monitor>Class of Service>Classifiers** in the J-Web user interface, or enter the **show class-of-service classifier** command.

[Table 154 on page 1388](#) summarizes key output fields for CoS classifiers.

**Table 160: Summary of Key CoS Classifier Output Fields**

Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).
CoS Value Type	The classifiers are displayed by type: <ul style="list-style-type: none"> <li>• <b>dscp</b>—All classifiers of the DSCP type.</li> <li>• <b>dscp ipv6</b>—All classifiers of the DSCP IPv6 type.</li> <li>• <b>exp</b>—All classifiers of the MPLS EXP type.</li> <li>• <b>ieee-802.1</b>—All classifiers of the IEEE 802.1 type.</li> <li>• <b>inet-precedence</b>—All classifiers of the IP precedence type.</li> </ul>	
Index	Internal index of the classifier.	
Incoming CoS Value	CoS value of the incoming packets, in bits. These values are used for classification.	
Assign to Forwarding Class	Forwarding class that the classifier assigns to an incoming packet. This class affects the forwarding and scheduling policies that are applied to the packet as it transits the device.	
Assign to Loss Priority	Loss priority value that the classifier assigns to the incoming packet based on its CoS value.	

- Related Documentation**
- [Monitoring CoS Interfaces on page 1387](#)
  - [Monitoring CoS Value Aliases on page 1389](#)
  - [Monitoring CoS RED Drop Profiles on page 1390](#)
  - [Monitoring CoS Forwarding Classes on page 1390](#)
  - [Monitoring CoS Rewrite Rules on page 1391](#)
  - [Monitoring CoS Scheduler Maps on page 1392](#)

## Monitoring Interfaces and Switching Functions

- [Displaying Real-Time Interface Information on page 1395](#)
- [Monitoring Address Pools on page 1397](#)
- [Monitoring Ethernet Switching on page 1398](#)



- [Monitoring GVRP on page 1399](#)
- [Monitoring Interfaces on page 1400](#)
- [Monitoring MPLS Traffic Engineering Information on page 1401](#)
- [Monitoring PPP on page 1406](#)
- [Monitoring PPPoE on page 1407](#)
- [Monitoring Spanning Tree on page 1410](#)
- [Monitoring the WAN Acceleration Interface on page 1411](#)

### 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 161 on page 1395](#) and [Table 162 on page 1395](#) list the keys you use to control the display using the **interface-name** and **traffic** options. (The keys are not case sensitive.)

**Table 161: 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.
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 162: CLI monitor interface traffic Output Control Keys**

Key	Action
b	Displays the statistics in units of bytes and bytes per second (bps).

Table 162: CLI monitor interface traffic Output Control Keys (*continued*)

Key	Action
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:
 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

```



**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 1400](#)

### 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 163 on page 1397](#) summarizes key output fields in the Address Pools page.

**Table 163: 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.	-
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.	-

Table 163: Address Pools Monitoring Page (*continued*)

Field	Values	Additional Information
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 1400](#)
  - [Threats Monitoring Report on page 1460](#)

### 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 164 on page 1398](#) summarizes the Ethernet Switching output fields.

Table 164: Summary of Ethernet Switching Output Fields

Field	Values	Additional Information
VLAN	The VLAN for which Ethernet Switching is enabled.	
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).	

Table 164: Summary of Ethernet Switching Output Fields (*continued*)

Field	Values	Additional Information
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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### [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 165 on page 1399](#) summarizes key output fields in the GVRP page.

Table 165: GVRP Monitoring Page

Field	Value	Additional Information
<b>Global GVRP Configuration</b>		
GVRP Status	Displays whether GVRP is enabled or disabled.	—
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.	—

Table 165: GVRP Monitoring Page (*continued*)

Field	Value	Additional Information
Protocol Status	Displays whether GVRP is enabled or disabled.	—

- Related Documentation**
- [Monitoring Ethernet Switching on page 1398](#)
  - [Monitoring Spanning Tree on page 1410](#)

### 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***

#### Related Documentation

- [Monitoring Overview on page 1283](#)
- [Monitoring Address Pools on page 1397](#)

### Monitoring MPLS Traffic Engineering Information

This section contains the following topics:

- [Monitoring MPLS Interfaces on page 1401](#)
- [Monitoring MPLS LSP Information on page 1402](#)
- [Monitoring MPLS LSP Statistics on page 1403](#)
- [Monitoring RSVP Session Information on page 1404](#)
- [Monitoring MPLS RSVP Interfaces Information on page 1405](#)

#### 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 166 on page 1402](#) summarizes key output fields in the MPLS interface information display.

Table 166: 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 167 on page 1402](#) summarizes key output fields in the MPLS LSP information display.

Table 167: 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.	–
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.



Table 167: Summary of Key MPLS LSP Information Output Fields (*continued*)

Field	Values	Additional Information
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 168 on page 1403 summarizes key output fields in the MPLS LSP statistics display.

Table 168: 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.

Table 168: Summary of Key MPLS LSP Statistics Output Fields (*continued*)

Field	Values	Additional 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 169 on page 1404](#) summarizes key output fields in the RSVP session information display.

Table 169: 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.	–
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.	–

Table 169: Summary of Key RSVP Session Information Output Fields (*continued*)

Field	Values	Additional Information
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 170 on page 1405](#) summarizes key output fields in the RSVP interfaces information display.

Table 170: 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.	—

Table 170: Summary of Key RSVP Interfaces Information Output Fields (*continued*)

Field	Values	Additional Information
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 1494](#)
  - [MPLS Connection Checking Overview on page 1492](#)
  - [Monitoring Overview on page 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### 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 1283](#)
- [Monitoring Interfaces on page 1400](#)

### 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 171 on page 1407](#) summarizes key output fields in PPPoE displays.

**Table 171: 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.
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.	—

Table 171: Summary of Key PPPoE Output Fields (*continued*)

Field	Values	Additional Information
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.	—
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.	—

Table 171: Summary of Key PPPoE Output Fields (*continued*)

Field	Values	Additional Information
Received	Number of the specific type of packet received by the PPPoE client.	—
Timeout	<p>Information about the timeouts that occurred during the PPPoE session.</p> <ul style="list-style-type: none"> <li>PADI—Number of timeouts that occurred for the PADI packet.</li> <li>PADO—Number of timeouts that occurred for the PADO packet. (This value is always 0 and is not supported.)</li> <li>PADR—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.	—
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 1283](#)
  - [Monitoring Interfaces on page 1400](#)
  - [Monitoring DHCP Client Bindings on page 1447](#)

### 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 172 on page 1410](#) summarizes key output fields in the spanning tree page.

**Table 172: 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.	—



Table 172: Spanning Tree Monitoring Page (*continued*)

Field	Value	Additional Information
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.	—
Role	MSTP or RSTP port role. Designated (DESG), backup (BKUP), alternate (ALT), or root.	—

- Related Documentation**
- [Monitoring Ethernet Switching on page 1398](#)
  - [Monitoring GVRP on page 1399](#)

### 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

## Monitoring NAT

- [Monitoring NAT on page 1412](#)

## Monitoring NAT

This section contains the following topics:

- [Monitoring Source NAT Information on page 1412](#)
- [Monitoring Destination NAT Information on page 1417](#)
- [Monitoring Static NAT Information on page 1419](#)
- [Monitoring Incoming Table Information on page 1421](#)
- [Monitoring Interface NAT Port Information on page 1422](#)

### 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 173 on page 1412](#) describes the available options for monitoring source NAT.

**Table 173: Source NAT Monitoring Page**

Field	Description	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 .	—
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.	—

Table 173: Source NAT Monitoring Page (*continued*)

Field	Description	Action
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/ Failed/ 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.	—
<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.	—

Table 173: Source NAT Monitoring Page (*continued*)

Field	Description	Action
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.	—
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.

Table 173: Source NAT Monitoring Page (*continued*)

Field	Description	Action
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.	—
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.	—

Table 173: Source NAT Monitoring Page (*continued*)

Field	Description	Action
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.	—
Port overloading factor	Port overloading capacity for PAT pools.	—
Address	Addresses in the pool.	—
Used	Number of used resources in the pool.  For Non-PAT pools, the number of used IP addresses is displayed.  For PAT pools, the number of used ports is displayed.	—

Table 173: Source NAT Monitoring Page (*continued*)

Field	Description	Action
Available	Number of available resources in the pool.  For Non-PAT pools, the number of available IP addresses is displayed.  For PAT pools, the number of available ports is displayed.	—
Total	Number of used and available resources in the pool.  For Non-PAT pools, the total number of used and available IP addresses is displayed.  For PAT pools, the total number of used and available ports is displayed.	—
Usage	Percent of resources used.  For Non-PAT pools, the percent of IP addresses used is displayed.  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.	—
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 174 on page 1418](#) summarizes key output fields in the destination NAT display.

**Table 174: 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.	—
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.	—



Table 174: Summary of Key Destination NAT Output Fields (*continued*)

Field	Values	Action
Sessions (Succ/ Failed/ 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 175 on page 1420 summarizes key output fields in the static NAT display.

**Table 175: 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.	—
Alarm threshold	Utilization alarm threshold.	—
Sessions (Succ/ Failed/ 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>	—

Table 175: Summary of Key Static NAT Output Fields (*continued*)

Field	Values	Action
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 176 on page 1421](#) summarizes key output fields in the incoming table display.

Table 176: Summary of Key Incoming Table Output Fields

Field	Values	Additional Information
<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.	—
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 177 on page 1422 summarizes key output fields in the interface NAT display.

**Table 177: 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

## Monitoring Security Policies

- [Monitoring Policy Statistics on page 1422](#)
- [Monitoring Routing Information on page 1423](#)
- [Monitoring Security Events by Policy on page 1430](#)
- [Monitoring Security Features on page 1432](#)

### 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 1543](#)
- [Checking a Security Policy Commit Failure on page 1544](#)
- [Verifying a Security Policy Commit on page 1544](#)
- [Debugging Policy Lookup on page 1544](#)

### Monitoring Routing Information

This section contains the following topics:

- [Monitoring Route Information on page 1423](#)
- [Monitoring RIP Routing Information on page 1425](#)
- [Monitoring OSPF Routing Information on page 1426](#)
- [Monitoring BGP Routing Information on page 1428](#)

#### **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 178 on page 1424 describes the different filters, their functions, and the associated actions.

Table 179 on page 1425 summarizes key output fields in the routing information display.

**Table 178: 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 179: 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.
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 180 on page 1426](#) summarizes key output fields in the RIP routing display in the J-Web user interface.

Table 180: 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.	—
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 181 on page 1427](#) summarizes key output fields in the OSPF routing display in the J-Web user interface.

**Table 181: 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.	—

Table 181: Summary of Key OSPF Routing Output Fields (*continued*)

Field	Values	Additional Information
Interface	Interface through which the neighbor is reachable.	–
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 182 on page 1429](#) summarizes key output fields in the BGP routing display in the J-Web user interface.

Table 182: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
<b>BGP Peer Summary</b>		
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 182: 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

### 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 183 on page 1430](#) describes the content of this pane.

Table 183: 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.

Table 183: View Policy Log Fields (*continued*)

Field	Value
Destination address	Destination address of the traffic that triggered the event.
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 184 on page 1432](#) describes the contents of this pane.

Table 184: 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 1283](#)
- [Monitoring Interfaces on page 1400](#)
- [Monitoring Alarms on page 1319](#)
- [Monitoring Events on page 1447](#)

#### Monitoring Security Features

This section contains the following topics:

- [Monitoring Policies on page 1432](#)
- [Checking Policies on page 1435](#)
- [Monitoring Screen Counters on page 1438](#)
- [Monitoring IDP Status on page 1440](#)
- [Monitoring Flow Gate Information on page 1441](#)
- [Monitoring Firewall Authentication Table on page 1442](#)
- [Monitoring Firewall Authentication History on page 1444](#)
- [Monitoring 802.1x on page 1446](#)

#### 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 185 on page 1433](#) 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 185: 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 185: 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 185: 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 186 on page 1436](#) 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 186: 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 186: Check Policies Output (*continued*)

Field	Function
Protocol	Name or equivalent value of the protocol to be matched.  ah—51 egp—8 esp—50 gre—47 icmp—1 igmp—2 igp—9 ipip—94 ipv6—41 ospf—89 pgm—113 pim—103 rdp—27 rsvp—46 sctp—132 tcp—6 udp—17 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 186: 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 187 on page 1438](#) summarizes key output fields in the screen counters display.

Table 187: 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 187: 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 187: 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 188 on page 1441](#) summarizes key output fields in the IDP display.

Table 188: 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 189 on page 1442](#) summarizes key output fields in the flow gate display.

Table 189: 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 190 on page 1443](#) summarizes key output fields in firewall authentication table display.



Table 190: 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 190: 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 191 on page 1444](#) summarizes key output fields in firewall authentication history display.

Table 191: 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 191: 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 191: 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 192 on page 1446](#) summarizes the Dot1X output fields.

Table 192: 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>		
MAC Address	MAC address of the authentication-failed host.	–

Table 192: Summary of Dot1X Output Fields (*continued*)

Field	Values	Additional Information
User Name	Name of the authentication-failed user.	–

- Related Documentation**
- [Monitoring Overview on page 1283](#)
  - [Monitoring Interfaces on page 1400](#)

## Monitoring Events, Services and System

- [Monitoring DHCP Client Bindings on page 1447](#)
- [Monitoring Events on page 1447](#)
- [Monitoring the System on page 1450](#)

### 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 193 on page 1447](#) summarizes the key output fields in the DHCP client binding displays.

Table 193: 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 1407](#)
  - [Understanding DHCP Client Operation on page 935](#)

### 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 194 on page 1448 summarizes key output fields in the events page.

**Table 194: 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 194: 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 1319](#)
  - [Monitoring Security Events by Policy on page 1430](#)

## 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 1450](#)
- [Monitoring Chassis Information on page 1452](#)
- [System Health Management for Branch SRX Series Devices on page 1454](#)

### *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 may 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

## Monitoring Unified Threat Management Features

- [Monitoring Antivirus Scan Engine Status on page 1455](#)
- [Monitoring Antivirus Scan Results on page 1456](#)
- [Monitoring Antivirus Session Status on page 1458](#)
- [Monitoring Content Filtering Configurations on page 1459](#)
- [Monitoring Reports on page 1459](#)
- [Monitoring Web Filtering Configurations on page 1466](#)

---

### 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/SRX210
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 1458](#)
- [Monitoring Antivirus Scan Results on page 1456](#)

---

### 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 1458](#)

---

### 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 1455](#)  
• [Monitoring Antivirus Scan Results on page 1456](#)



## 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 FilteringMonitor>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 1460](#)
- [Traffic Monitoring Report on page 1464](#)

### ***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 195 on page 1460](#) for a description of the page content.
  - **Activities** tab. See [Table 196 on page 1462](#) for a description of the page content.

**Table 195: Statistics Tab Output in the Threats Report**

Field	Description
<b>General Statistics Pane</b>	
Threat Category	<p>One of the following categories of threats:</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—Click the Web filter category to display counters for 39 subcategories.</li> <li>• Content Filter</li> </ul> </li> <li>• Firewall Event</li> </ul>
Severity	<p>Severity level of the 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>
Hits in past 24 hours	Number of threats encountered per category in the past 24 hours.

Table 195: Statistics Tab Output in the Threats Report (*continued*)

Field	Description
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.
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.

Table 195: Statistics Tab Output in the Threats Report (*continued*)

Field	Description
<b>Threat Trend in past 24 hours</b>	
Category	Pie chart graphic representing comparative threat counts by category: <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>
<b>Web Filter Counters Summary</b>	
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 196: Activities Tab Output in the Threats Report

Field	Function
<b>Most Recent Virus Hits</b>	
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	Severity level 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 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 196: 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 196: 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 197 on page 1464](#) for a description of the report.

Table 197: 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 197: 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

---

### 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 1467](#)



## Monitoring VPNs

This section contains the following topics:

- [Monitoring IKE Gateway Information on page 1467](#)
- [Monitoring IPsec VPN—Phase I on page 1470](#)
- [Monitoring IPsec VPN—Phase II on page 1471](#)
- [Monitoring IPsec VPN Information on page 1472](#)

### 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 198 on page 1467](#) summarizes key output fields in the IKE gateway display.

**Table 198: Summary of Key IKE SA Information Output Fields**

Field	Values	Additional Information
<b>IKE Security Associations</b>		
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.	—
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.

Table 198: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
Mode	<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>	—
<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	<p>State of the IKE security associations:</p> <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.

Table 198: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
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.	—
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>	—

Table 198: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
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.	—
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 199 on page 1470](#) describes the available options for monitoring IPsec VPN-Phase I.

Table 199: IPsec VPN—Phase I Monitoring Page

Field	Values	Additional Information
<b>IKE SA Tab Options</b>		
<b>IKE Security Associations</b>		
SA Index	Index number of an SA.	—
Remote Address	IP address of the destination peer with which the local peer communicates.	—

Table 199: IPsec VPN—Phase I Monitoring Page (*continued*)

Field	Values	Additional Information
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.
Mode	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: <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 200 on page 1471](#) describes the available options for monitoring IPsec VPN-Phase II.

Table 200: IPsec VPN—Phase II Monitoring Page

Field	Values	Additional Information
Statistics Tab Details		

Table 200: IPsec VPN—Phase II Monitoring Page (*continued*)

Field	Values	Additional Information
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.	—
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	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.	—
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 201 on page 1473 summarizes key output fields in the IPsec VPN display.

**Table 201: Summary of Key IPsec VPN Information Output Fields**

Field	Values	Additional Information
<b>IPsec Security Associations</b>		
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	Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations: <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	State has two options, <b>Installed</b> and <b>Not Installed</b> . <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> .

Table 201: Summary of Key IPsec VPN Information Output Fields (*continued*)

Field	Values	Additional Information
Vsys	The root system.	—
<b>IPsec Statistics Information</b>		
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>	—



Table 201: Summary of Key IPsec VPN Information Output Fields (*continued*)

Field	Values	Additional Information
Details for IPsec SA Index: <i>ID</i>		
Virtual System	The root system.	—
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 201: 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 201: 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 1283](#)
  - [Monitoring Interfaces on page 1400](#)

## Troubleshooting

- [Configuring Data Path Debugging and Trace Options on page 1477](#)
- [Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits on page 1491](#)
- [Using Packet Capture to Analyze Network Traffic on page 1508](#)
- [Troubleshooting Security Devices on page 1531](#)

## Configuring Data Path Debugging and Trace Options

- [Understanding Data Path Debugging for SRX Series Devices on page 1477](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1479](#)
- [Example: Configuring End-to-End Debugging on a High-End SRX Series Device on page 1479](#)
- [Understanding Security Debugging Using Trace Options on page 1483](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1483](#)
- [Displaying Log and Trace Files on page 1485](#)
- [Displaying Output for Security Trace Options on page 1485](#)
- [Displaying Multicast Trace Operations on page 1486](#)
- [Using the J-Web Traceroute Tool on page 1486](#)
- [J-Web Traceroute Results and Output Summary on page 1488](#)
- [Understanding Flow Debugging Using Trace Options on page 1489](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1489](#)
- [Displaying a List of Devices on page 1490](#)

### 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 1483](#)
- [Understanding Flow Debugging Using Trace Options on page 1489](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1479](#)
- [Example: Configuring End-to-End Debugging on a High-End SRX Series Device on page 1479](#)

### 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
```

3. 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
```

4. 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 1477](#)
- [Understanding Security Debugging Using Trace Options on page 1483](#)
- [Understanding Flow Debugging Using Trace Options on page 1489](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1489](#)

### 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 1479](#)
- [Overview on page 1480](#)
- [Configuration on page 1480](#)
- [Enabling Data Path Debugging on page 1482](#)
- [Verification on page 1482](#)

#### 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* 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 succesfully 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 1477](#)

### 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 1477](#)
- [Understanding Flow Debugging Using Trace Options on page 1489](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1483](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1479](#)
- [Displaying Output for Security Trace Options on page 1485](#)

### 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 1483](#)
- [Displaying Output for Security Trace Options on page 1485](#)

### 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 1490](#)
  - [Displaying Real-Time Monitoring Information on page 1360](#)

### 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 1483](#)
  - [Setting Security Trace Options \(CLI Procedure\) on page 1483](#)

## 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 202 on page 1486 summarizes the output fields of the display.

Table 202: CLI mtrace monitor Command Output Summary

Field	Description
<i>Mtrace operation-type at time-of-day</i>	<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>
<i>by</i>	IP address of the host issuing the query.
<i>resp to address</i>	<b>address</b> —Response destination address.
<i>qid qid</i>	<b>qid</b> —Query ID number.
<i>packet from source to destination</i>	<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>
<i>from source to destination</i>	<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>
<i>via group address</i>	<b>address</b> —Group address being traced.
<i>mxhop=number</i>	<b>number</b> —Maximum hop setting.

- Related Documentation**
- [Using the J-Web Traceroute Tool on page 1486](#)
  - [J-Web Traceroute Results and Output Summary on page 1488](#)

## 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 203 on page 1487](#)).

**Table 203: Traceroute Field Summary**

Field	Function	Your Action
Remote Host	Identifies the destination host of the traceroute.  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	<p>Determines whether traceroute packets are routed by means of the routing table.</p> <p>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.</p>	<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.

Table 203: Traceroute Field Summary (*continued*)

Field	Function	Your Action
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 1284](#)
- [J-Web Traceroute Results and Output Summary on page 1488](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)
- *Interfaces Feature Guide for Security Devices*

#### J-Web Traceroute Results and Output Summary

Table 204 on page 1488 summarizes the output in the traceroute display.

Table 204: 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.

Table 204: J-Web Traceroute Results and Output Summary (*continued*)

Field	Description
<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 1284](#)
- [Using the J-Web Traceroute Tool on page 1486](#)
- [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 1477](#)
- [Understanding Security Debugging Using Trace Options on page 1483](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1489](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1479](#)

#### 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 1489](#)

### 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 205 on page 1490](#) describes the **traceroute** command options.

**Table 205: 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.



Table 205: CLI traceroute Command Options (*continued*)

Option	Description
<b>bypass-routing</b>	(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.  Use this option to display a route to a local system through an interface that has no route through it.
<b>gateway address</b>	(Optional) Uses the gateway you specify to route through.
<b>inet</b>	(Optional) Forces the traceroute packets to an IPv4 destination.
<b>inet6</b>	(Optional) Forces the traceroute packets to an IPv6 destination.
<b>no-resolve</b>	(Optional) Suppresses the display of the hostnames of the hops along the path.
<b>routing-instance</b> <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 1485](#)

## Using MPLS to Diagnose LSPs, VPNs, and Layer 2 Circuits

- [MPLS Connection Checking Overview on page 1492](#)
- [Configuring Ping MPLS on page 1494](#)
- [Using the ping Command on page 1494](#)

- [Using the J-Web Ping Host Tool on page 1496](#)
- [J-Web Ping Host Results and Output Summary on page 1498](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- [J-Web Ping MPLS Results and Output Summary on page 1502](#)
- [Pinging Layer 2 Circuits on page 1503](#)
- [Pinging Layer 2 VPNs on page 1504](#)
- [Pinging Layer 3 VPNs on page 1506](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1507](#)

### 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 86 on page 655](#) 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 206: Options for Checking MPLS Connections**

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping RSVP-signaled LSP	<b>ping mpls rsvp</b>	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	<b>ping mpls ldp</b>	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.  Ping requests sent to LDP-signaled LSPs use only the master routing instance.

Table 206: Options for Checking MPLS Connections (*continued*)

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
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.	—
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 1284](#)
  - [Configuring Ping MPLS on page 1494](#)
  - [Using the J-Web Ping Host Tool on page 1496](#)
  - [Using the ping Command on page 1494](#)

## 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 1284](#)
- [MPLS Connection Checking Overview on page 1492](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- [Using the ping Command on page 1494](#)

## 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> <ttl number> <wait seconds> <detail> <verbose>
```

[Table 207 on page 1495](#) describes the **ping** command options.

To quit the **ping** command, press Ctrl-C.

Table 207: 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.  Use this option to ping a local system through an interface that has no route through it.
<i>countnumber</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.
<i>rapid</i>	(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.
<i>record-route</i>	(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.
<i>routing-instance routing-instance-name</i>	(Optional) Uses the routing instance you specify for the ping request.
<i>size bytes</i>	(Optional) Sets the size of the ping request packet. Specify a size from 0 through 65,468. The default value is 56 bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.
<i>source source-address</i>	(Optional) Uses the source address that you specify, in the ping request packet.
<i>strict</i>	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.

Table 207: CLI ping Command Options (*continued*)

Option	Description
<b>strict-source</b> <i>[hosts]</i>	(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 1284](#)
- [Configuring Ping MPLS on page 1494](#)
- [Pinging Layer 2 Circuits on page 1503](#)
- [Pinging Layer 2 VPNs on page 1504](#)
- [Pinging Layer 3 VPNs on page 1506](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1507](#)
- [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 1494](#).)

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 208 on page 1497](#)).

**Table 208: J-Web Ping Host Field Summary**

Field	Function	Your Action
Remote Host	Identifies the host to ping.  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>
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.

Table 208: J-Web Ping Host Field Summary (*continued*)

Field	Function	Your Action
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 1284](#)
- [Configuring Ping MPLS on page 1494](#)
- [J-Web Ping Host Results and Output Summary on page 1498](#)
- [Using the J-Web Traceroute Tool on page 1486](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)

**J-Web Ping Host Results and Output Summary**

Table 209 on page 1498 summarizes the output in the ping host display.

Table 209: 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> <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.



Table 209: Ping Host Results and Output (*continued*)

Ping Host Result	Description
<i>percentage packet loss</i>	<i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage.
<i>round-trip min/avg/max/stddev = min-time/avg-time/max-time/std-dev ms</i>	<ul style="list-style-type: none"> <li><i>min-time</i>—Minimum round-trip time (see <i>time=time</i> field in this table).</li> <li><i>avg-time</i>—Average round-trip time.</li> <li><i>max-time</i>—Maximum round-trip time.</li> <li><i>std-dev</i>—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 1284](#)
- [Configuring Ping MPLS on page 1494](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- *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 210 on page 1500](#)).

Table 210: 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.
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.

Table 210: 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>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.
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.

Table 210: 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.
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 1284](#)
- [Configuring Ping MPLS on page 1494](#)
- [J-Web Ping MPLS Results and Output Summary on page 1502](#)
- [Using the J-Web Traceroute Tool on page 1486](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)

#### J-Web Ping MPLS Results and Output Summary

Table 211 on page 1502 summarizes the output in the ping MPLS display.

Table 211: 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.

Table 211: J-Web Ping MPLS Results and Output Summary (*continued*)

Field	Description
<i>number</i> packets transmitted	<i>number</i> —Number of ping requests (probes) sent to a host.
<i>number</i> packets received	<i>number</i> —Number of ping responses received from a host.
<i>percentage</i> packet loss	<i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage.
time	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 1284](#)
- [Configuring Ping MPLS on page 1494](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- *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 212 on page 1504](#) describes the **ping mpls l2circuit** command options.

Table 212: CLI ping mpls l2circuit Command Options

Option	Description
<b>l2circuit interface</b> <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 neighbor</b> <i>prefix-name</i> <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>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 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 1494](#)
- [Configuring Ping MPLS on page 1494](#)
- [Pinging Layer 2 VPNs on page 1504](#)
- [Pinging Layer 3 VPNs on page 1506](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1507](#)
- [Using the J-Web Ping Host Tool on page 1496](#)

#### 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 213 on page 1505](#) describes the **ping mpls l2vpn** command options.

Table 213: CLI ping mpls l2vpn Command Options

Option	Description
<b>l2vpn interface</b> <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> <i>l2vpn-instance-name</i> <i>local-site-id</i> <i>local-site-id-number</i> <i>remote-site-id</i> <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

--- 1sping 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 1494](#)
- [Configuring Ping MPLS on page 1494](#)
- [Pinging Layer 2 Circuits on page 1503](#)
- [Pinging Layer 3 VPNs on page 1506](#)

- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1507](#)
- [Using the J-Web Ping Host Tool on page 1496](#)

### 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 214 on page 1506](#) describes the **ping mpls l3vpn** command options.

**Table 214: 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
!!!!
--- 1sping 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 1494](#)
- [Configuring Ping MPLS on page 1494](#)
- [Pinging Layer 2 Circuits on page 1503](#)
- [Pinging Layer 2 VPNs on page 1504](#)



- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1507](#)
- [Using the J-Web Ping Host Tool on page 1496](#)

### 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 215 on page 1507](#) describes the **ping mpls** command options.

**Table 215: 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 1494](#)
- [Configuring Ping MPLS on page 1494](#)
- [Pinging Layer 2 Circuits on page 1503](#)
- [Pinging Layer 2 VPNs on page 1504](#)

- [Pinging Layer 3 VPNs on page 1506](#)
- [Using the J-Web Ping Host Tool on page 1496](#)

## Using Packet Capture to Analyze Network Traffic

- [Packet Capture Overview on page 1508](#)
- [Example: Enabling Packet Capture on a Device on page 1511](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Example: Configuring Packet Capture for Datapath Debugging on page 1518](#)
- [Disabling Packet Capture on page 1521](#)
- [Deleting Packet Capture Files on page 1521](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1522](#)
- [Displaying Packet Headers on page 1523](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)
- [J-Web Packet Capture Results and Output Summary on page 1530](#)

### 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 1509](#)
- [Firewall Filters for Packet Capture on page 1510](#)
- [Packet Capture Files on page 1510](#)
- [Analysis of Packet Capture Files on page 1510](#)

### ***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 1511](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)

- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)

### 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 1511](#)
- [Overview on page 1511](#)
- [Configuration on page 1511](#)
- [Verification on page 1512](#)

#### Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1512](#)
- [Verifying Captured Packets on page 1512](#)

### **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 -xvvvvv
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
root@server%

```

#### Related Documentation

- [Packet Capture Overview on page 1508](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Disabling Packet Capture on page 1521](#)
- [Deleting Packet Capture Files on page 1521](#)
- [Disabling Packet Capture on page 1521](#)

#### Example: Configuring Packet Capture on an Interface

This example shows how to configure packet capture on an interface to analyze traffic.

- [Requirements on page 1514](#)
- [Overview on page 1514](#)
- [Configuration on page 1515](#)
- [Verification on page 1515](#)

#### Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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**

**Purpose** Confirm that the configuration is working properly.  
 Verify that packet capture is configured on the interface.

**Action** From configuration mode, enter the **show interfaces fe-0/0/1** command.

- Related Documentation**
- [Packet Capture Overview on page 1508](#)
  - [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1522](#)
  - [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
  - [Example: Enabling Packet Capture on a Device on page 1511](#)
  - [Deleting Packet Capture Files on page 1521](#)
  - [Disabling Packet Capture on page 1521](#)

### 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 1516](#)
- [Overview on page 1516](#)
- [Configuration on page 1516](#)
- [Verification on page 1517](#)

#### Requirements

Before you begin:

- Establish basic connectivity. See the *Getting Started Guide for Branch SRX Series* for your device.
- 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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*.

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 1508](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Enabling Packet Capture on a Device on page 1511](#)
- [Deleting Packet Capture Files on page 1521](#)
- [Disabling Packet Capture on page 1521](#)

### 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 1518](#)
- [Overview on page 1518](#)
- [Configuration on page 1518](#)
- [Verification on page 1520](#)

#### Requirements

Before you begin, see “[Debugging the Data Path \(CLI Procedure\)](#)” on page 1479.

#### 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, and then 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* 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 1520](#)
- [Verifying Data Path Debugging Capture on page 1520](#)
- [Verifying Data Path Debugging Counter on page 1520](#)

### **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 1508](#)
- [Understanding Data Path Debugging for SRX Series Devices on page 1477](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1479](#)

### 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 1508](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Example: Enabling Packet Capture on a Device on page 1511](#)
- [Deleting Packet Capture Files on page 1521](#)

### 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 1521](#)).
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 1511](#)).
4. If you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [Packet Capture Overview on page 1508](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Example: Enabling Packet Capture on a Device on page 1511](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1522](#)
- [Disabling Packet Capture on page 1521](#)

### 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 reenable 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 1521](#)).
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 1511](#)).
7. If you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [Packet Capture Overview on page 1508](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1516](#)
- [Example: Enabling Packet Capture on a Device on page 1511](#)

#### 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 216 on page 1523](#) describes the **monitor traffic** command options.

**Table 216: 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 <b>0</b> through <b>100,000</b> . 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.

Table 216: CLI monitor traffic Command Options (*continued*)

Option	Description
<b>matching "expression"</b>	(Optional) Displays packet headers that match an expression enclosed in quotation marks (" "). <a href="#">Table 217 on page 1525</a> through <a href="#">Table 219 on page 1527</a> 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.  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.
<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 217 on page 1525](#), enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in [Table 218 on page 1526](#) (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 219 on page 1527](#) (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in [Table 219 on page 1527](#).
- Binary—Expressions that use the binary operators listed in [Table 219 on page 1527](#).
- Packet data accessor—Expressions that use the following syntax:

```
protocol [byte-offset <size>]
```

Replace *protocol* with any protocol in [Table 217 on page 1525](#). 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 217: 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 address</b>	Matches packet headers with source or destination addresses containing the specified network address.
<b>network address mask</b> <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 bytes</b>	Matches packets with lengths less than or equal to the specified value, in bytes.
<b>greater bytes</b>	Matches packets with lengths greater than or equal to the specified value, in bytes.

Table 217: CLI monitor traffic Match Conditions (*continued*)

Match Condition	Description
<b>Protocol</b>	
<b>arp</b>	Matches all ARP packets.
<b>ether</b>	Matches all Ethernet frames.
<b>ether [broadcast   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 [address   (\arp   \ip   \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 [broadcast   multicast]</b>	Matches broadcast or multicast IP packets.
<b>ip protocol [address   (\icmp   igmp   \tcp   \udp)]</b>	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 218: 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 219: CLI monitor traffic Arithmetic, Binary, and Relational Operators

Operator	Description
<b>Arithmetic Operator</b>	
+	Addition operator.
–	Subtraction operator.
/	Division operator.
<b>Binary Operator</b>	
&	Bitwise AND.
*	Bitwise exclusive OR.
	Bitwise inclusive OR.
<b>Relational Operator</b>	
<=	A match occurs if the first expression is less than or equal to the second.
>=	A match occurs if the first expression is greater than or equal to the second.
<	A match occurs if the first expression is less than the second.
>	A match occurs if the first expression is greater than the second.
=	A match occurs if the first expression is equal to the second.
!=	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 1508](#)
- [Using the J-Web Packet Capture Tool on page 1527](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1522](#)
- [Example: Configuring Packet Capture on an Interface on page 1514](#)

#### 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 220 on page 1528](#)). 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 220: Packet Capture Field Summary**

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured.  If you select <b>default</b> , packets on the Ethernet management port 0 are captured.	Select an interface from the list—for example, <b>ge-0/0/0</b> .
Detail level	Specifies the extent of details to be displayed for the packet headers.  <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	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.	Select the number of packets to be captured from the list—for example, <b>10</b> .

Table 220: Packet Capture Field Summary (*continued*)

Field	Function	Your Action
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>From the Direction list, select <b>source</b>.</li> <li>From the Type list, select <b>host</b>.</li> <li>In the Address box, type <b>10.1.40.48</b>.</li> <li>Click <b>Add</b>.</li> </ol>
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.	<p>Select a direction and a port. For example:</p> <ol style="list-style-type: none"> <li>From the Type list, select <b>src</b>.</li> <li>In the Port box, type <b>23</b>.</li> </ol>
<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>

Table 220: Packet Capture Field Summary (*continued*)

Field	Function	Your Action
Header Expression	Specifies the match condition for the packets to capture.  The match conditions you specify for Addresses, Protocols, and Ports appear in expression format in this field.	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> .
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	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> .  If you select this option, the decoded packet headers do not appear on the packet capture page.	<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 1508](#)
- [Diagnostic Tools Overview on page 1284](#)
- [J-Web Packet Capture Results and Output Summary on page 1530](#)
- [Using the J-Web Ping MPLS Tool on page 1499](#)
- [Using the J-Web Ping Host Tool on page 1496](#)
- [Using the J-Web Traceroute Tool on page 1486](#)

### [J-Web Packet Capture Results and Output Summary](#)

[Table 221 on page 1531](#) summarizes the output in the packet capture display.



Table 221: J-Web Packet Capture Results and Output Summary

Field	Description
<i>timestamp</i>	Time when the packet was captured. The timestamp <b>00:45:40.823971</b> means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds.  <b>NOTE:</b> The time displayed is local time.
<i>direction</i>	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> ).
<i>protocol</i>	Protocol for the packet.  In the sample output, <b>IP</b> indicates the Layer 3 protocol.
<i>source address</i>	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.  <b>NOTE:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.
<i>destination address</i>	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.  <b>NOTE:</b> When a string is defined for the port, the packet capture output displays the string instead of the port number.
<i>protocol</i>	Protocol for the packet.  In the sample output, <b>TCP</b> indicates the Layer 4 protocol.
<i>data size</i>	Size of the packet (in bytes).

- Related Documentation**
- [Packet Capture Overview on page 1508](#)
  - [Diagnostic Tools Overview on page 1284](#)
  - [Using the J-Web Packet Capture Tool on page 1527](#)

## Troubleshooting Security Devices

- [Recovering the Root Password for SRX Series Devices on page 1532](#)
- [Troubleshooting Access Manager Client-Side Problems on page 1533](#)
- [Troubleshooting DNS Name Resolution in Logical System Security Policies \(Master Administrators Only\) on page 1533](#)
- [Troubleshooting the Link Services Interface on page 1534](#)
- [Troubleshooting Security Policies on page 1543](#)
- [Troubleshooting ISSU-Related Problems Using Log Error Messages on page 1545](#)

## 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 Access Manager Client-Side Problems

---

**Problem**     **Description:** Users are having problems connecting to the remote access server using Access Manager.

**Solution**     Use the following tools to troubleshoot client-side issues:

- Client-side logs—To view client-side logs, open Access Manager and choose **Save logs and diagnostics** from the File menu. Select a location on your computer to save the zipped log files and click **Save**.
- Detailed logs—To create more detailed client-side logs, open Access Manager and choose **Enable Detailed Logging** from the File menu.
- Firewall connection information—To view connection information for a given firewall, open Access Manager, right-click to select the firewall, and choose **Status**.

**Related Documentation**

- *Understanding Remote Client Access to the VPN*
- *Access Manager Client-Side System Requirements*
- *Access Manager Client-Side Files*
- *Access Manager Client-Side Registry Changes*
- *Access Manager Client-Side Error 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 may 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 may 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](#)
- [Example: Configuring Logical Systems Security Profiles \(Master Administrators Only\)](#)
- [show security dns-cache](#)
- [clear security dns-cache](#)
- [show security policies on page 102](#)

---

### 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 1534](#)
- [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1536](#)
- [Determine If LFI and Load Balancing Are Working Correctly on page 1536](#)

#### ***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 222 on page 1535](#) shows the CoS components to be applied on a multilink bundle and its constituent links.

**Table 222: 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.

Table 222: CoS Components Applied on Multilink Bundles and Constituent Links (*continued*)

Cos Component	Multilink Bundle	Constituent Links	Explanation
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.
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. See *Example: Configuring Interface Shaping Rates*.
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. For more information, see *Verifying the Link Services Interface*.

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. See *Example: Configuring Link Fragmentation and Interleaving*.



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.

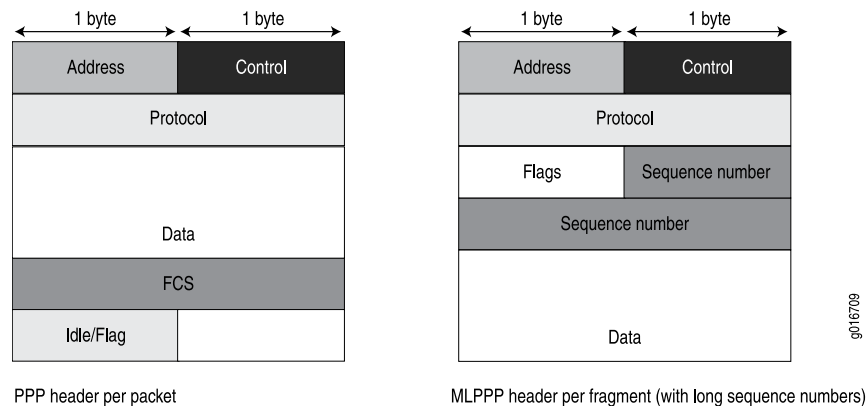
A small unfragmented data packet contains a PPP header and a single MLPPP header. In a large fragmented data packet, the first fragment contains a PPP header and an MLPPP header, but the consecutive fragments contain only an MLPPP header.

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 59 on page 1539 shows the overhead added to PPP and MLPPP headers.

**Figure 59: 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 223 on page 1539 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 223: 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 223: 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 224 on page 1542](#) 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 224: Number of Packets Transmitted on a Queue**

Packets Queued	Bundle lsq-0/0/0.0	Constituent Link se-1/0/0	Constituent Link 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. For more information, see *Example: Configuring Scheduler Maps*.
- 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.

---

### Troubleshooting Security Policies

- [Synchronizing Policies Between Routing Engine and Packet Forwarding Engine on page 1543](#)
- [Checking a Security Policy Commit Failure on page 1544](#)
- [Verifying a Security Policy Commit on page 1544](#)
- [Debugging Policy Lookup on page 1544](#)

#### *Synchronizing Policies Between Routing Engine and Packet Forwarding Engine*

**Problem**     **Description:** Security policies are stored in both the Routing Engine and the Packet Forwarding Engine. After you modify a policy, you commit the configuration on the Routing Engine, and it is synchronized to the Packet Forwarding Engine.

**Environment:** The policies in the Routing Engine and Packet Forwarding Engine must be in sync for the configuration to be committed. However, under certain circumstances, policies in the Routing Engine and the Packet Forwarding Engine might be out of sync, which causes the commit to fail.

**Symptoms:** The following error message appears if you attempt to commit a configuration when the policies in the Routing Engine and Packet Forwarding Engine are out of sync:  
**Policy is out of sync between RE and PFE <SPU-name(s)> Please resync before commit.**

**Solution**     Synchronize the policies as follows:

- Reboot the device (standalone)
- Reboot the devices (chassis cluster)

### ***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 on page 1543](#)
  - [Checking a Security Policy Commit Failure on page 1544](#)
  - [Verifying a Security Policy Commit on page 1544](#)
  - [Debugging Policy Lookup on page 1544](#)

---

### Troubleshooting ISSU-Related Problems Using Log Error Messages

---

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 1545](#)
- [Kernel State Synchronization on page 1545](#)
- [Installation Related Errors on page 1545](#)
- [ISSU Support Related Errors on page 1546](#)
- [RG Groups Failover Errors on page 1546](#)
- [Initial Validation Checks Fail on page 1546](#)

#### ***Chassisd Process Errors***

**Problem Description:** There are 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:** There are 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:** There is an 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
```

#### *RG Groups Failover Errors*

**Problem** **Description:** There is a problem with automatic redundancy group 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 Failures*

### Configuration Statements and Operational Commands

- [Configuration Statements on page 1548](#)
- [Operational Commands on page 1603](#)

## Configuration Statements

- [Chassis Configuration Statement Hierarchy on page 1549](#)
- [Accounting-Options Configuration Statement Hierarchy on page 1552](#)
- [\[edit security\] Hierarchy Level on page 1554](#)
- [\[edit security alarms\] Hierarchy Level on page 1555](#)
- [\[edit security datapath-debug\] Hierarchy Level on page 1556](#)
- [\[edit security traceoptions\] Hierarchy Level on page 1557](#)
- [accounting-options on page 1557](#)
- [action-profile on page 1558](#)
- [archive-sites on page 1559](#)
- [capture-file \(Security\) on page 1560](#)
- [class-usage-profile on page 1561](#)
- [cluster \(Chassis\) on page 1562](#)
- [counters on page 1563](#)
- [datapath-debug on page 1564](#)
- [decryption-failures on page 1565](#)
- [destination-classes on page 1566](#)
- [destination-interface on page 1567](#)
- [destination-port on page 1568](#)
- [fields \(for Interface Profiles\) on page 1569](#)
- [fields \(for Routing Engine Profiles\) on page 1570](#)
- [file \(Associating with a Profile\) on page 1571](#)
- [file \(Configuring a Log File\) on page 1572](#)
- [files on page 1573](#)
- [filter-profile on page 1573](#)
- [flow \(Security Flow\) on page 1574](#)
- [global-threshold on page 1576](#)
- [global-weight on page 1577](#)
- [hardware-timestamp on page 1577](#)
- [icmp on page 1578](#)
- [idp \(Security Alarms\) on page 1578](#)
- [interface-profile on page 1579](#)
- [interval on page 1580](#)
- [ip-monitoring on page 1581](#)
- [ip-monitoring \(Services\) on page 1582](#)
- [maximum-capture-size \(Datapath Debug\) on page 1583](#)

- [mib-profile on page 1583](#)
- [mpls \(Security Forwarding Options\) on page 1584](#)
- [next-hop on page 1584](#)
- [nonpersistent on page 1585](#)
- [object-names on page 1585](#)
- [operation on page 1586](#)
- [packet-capture on page 1587](#)
- [packet-filter on page 1588](#)
- [probe on page 1589](#)
- [probe-interval on page 1590](#)
- [probe-limit on page 1590](#)
- [probe-server on page 1591](#)
- [probe-type on page 1592](#)
- [redundancy-group \(Chassis Cluster\) on page 1593](#)
- [retry-interval \(Chassis Cluster\) on page 1594](#)
- [routing-engine-profile on page 1595](#)
- [rpm \(Services\) on page 1596](#)
- [size on page 1598](#)
- [source-classes on page 1598](#)
- [start-time on page 1599](#)
- [target on page 1599](#)
- [thresholds on page 1600](#)
- [traceoptions \(Security Datapath Debug\) on page 1601](#)
- [transfer-interval on page 1602](#)
- [traps on page 1603](#)

---

### Chassis Configuration Statement Hierarchy

Use the statements in the **chassis** configuration hierarchy to configure alarms, aggregated devices, clusters, the Routing Engine, and other chassis properties.

```
chassis {
 aggregated-devices {
 ethernet {
 device-count number;
 lacp {
 link-protection {
 non-revertive;
 }
 system-priority number;
 }
 }
 }
 sonet {
 device-count number;
 }
}
```

```
 }
 }
 alarm {
 ds1 {
 ais (ignore | red | yellow);
 ylw (ignore | red | yellow);
 }
 ethernet {
 link-down (ignore | red | yellow);
 }
 integrated-services {
 failure (ignore | red | yellow);
 }
 management-ethernet {
 link-down (ignore | red | yellow);
 }
 serial {
 cts-absent (ignore | red | yellow);
 dcd-absent (ignore | red | yellow);
 dsr-absent (ignore | red | yellow);
 loss-of-rx-clock (ignore | red | yellow);
 loss-of-tx-clock (ignore | red | yellow);
 }
 services {
 hw-down (ignore | red | yellow);
 linkdown (ignore | red | yellow);
 pic-hold-reset (ignore | red | yellow);
 pic-reset (ignore | red | yellow);
 rx-errors (ignore | red | yellow);
 sw-down (ignore | red | yellow);
 tx-errors (ignore | red | yellow);
 }
 t3 {
 ais (ignore | red | yellow);
 exz (ignore | red | yellow);
 ferf (ignore | red | yellow);
 idle (ignore | red | yellow);
 lcv (ignore | red | yellow);
 lof (ignore | red | yellow);
 los (ignore | red | yellow);
 pll (ignore | red | yellow);
 ylw (ignore | red | yellow);
 }
 }
 cluster {
 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;
}
}
config-button {
 no-clear;
 no-rescue;
}
craft-lockout;
fpc slot-number {
 offline;
 pic slot-number {
 aggregate-ports;
 framing {
 (e1 | e3 | sdh | sonet | t1 | t3);
 }
 }
 max-queues-per-interface (4 | 8);
 mlfr-uni-nni-bundles number;
 no-multi-rate;
 port slot-number {
 framing (e1 | e3 | sdh | sonet | t1 | t3);
 }
}

```

```

 speed (oc12-stm4 | oc3-stm1 | oc48-stm16);
 }
 q-pic-large-buffer (large-scale | small-scale);
 services-offload {
 low-latency;
 per-session-statistics;
 }
 shdsl {
 pic-mode (1-port-atm | 2-port-atm | 4-port-atm | efm);
 }
 sparse-dlcis;
 traffic-manager {
 egress-shaping-overhead number;
 ingress-shaping-overhead number;
 mode (egress-only | ingress-and-egress);
 }
 tunnel-queuing;
}
services-offload;
}
ioc-npc-connectivity {
 ioc slot-number {
 npc (npc-slot-number | none);
 }
}
maximum-ecmp (16 | 32 | 64);
network-services (ethernet | IP);
routing-engine {
 bios {
 no-auto-upgrade;
 }
 on-disk-failure {
 disk-failure-action (halt | reboot);
 }
 usb-wwan {
 port 1;
 }
}
usb {
 storage {
 disable;
 }
}
}
}

```

- Related Documentation
- [cluster \(Chassis\) on page 1562](#)
  - [ip-monitoring on page 1581](#)

### Accounting-Options Configuration Statement Hierarchy

Use the statements in the **accounting-options** configuration hierarchy to collect and log data about basic system operations and services on the device.

```
accounting-options {
```

```

class-usage-profile profile-name {
 destination-classes {
 destination-class-name;
 }
 file filename;
 interval minutes;
 source-classes {
 source-class-name;
 }
}
file filename {
 archive-sites url {
 password password ;
 }
 files number;
 nonpersistent;
 size bytes;
 start-time yyyy-mm-dd.hh:mm;
 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 (get | get-next | walk) ;
}
periodic-refresh disable;
routing-engine-profile profile-name {
 fields {
 field-name ;
 }
 file filename;
 interval minutes;
}
}

```

**Related  
Documentation**

- [Administration Guide for Security Devices](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level](#)

### [\[edit security\] Hierarchy Level](#)

---

Each of the following topics lists the statements at a subhierarchy of the **[edit security]** hierarchy.

- [\[edit security alg\] Hierarchy Level](#)
- [\[edit security analysis\] Hierarchy Level](#)
- [\[edit security application-tracking\] Hierarchy Level](#)
- [\[edit security authentication-key-chains\] Hierarchy Level](#)
- [\[edit security certificates\] Hierarchy Level](#)
- [\[edit security datapath-debug\] Hierarchy Level](#)
- [\[edit security firewall-authentication\] Hierarchy Level](#)
- [\[edit security flow\] Hierarchy Level](#)
- [\[edit security forwarding-options\] Hierarchy Level](#)
- [\[edit security forwarding-process\] Hierarchy Level](#)
- [\[edit security gprs\] Hierarchy Level](#)
- [\[edit security group-vpn\] Hierarchy Level](#)
- [\[edit security idp\] Hierarchy Level](#)
- [\[edit security ike\] Hierarchy Level](#)
- [\[edit security ipsec\] Hierarchy Level](#)
- [\[edit security log\] Hierarchy Level](#)
- [\[edit security nat\] Hierarchy Level](#)
- [\[edit security pki\] Hierarchy Level](#)
- [\[edit security policies\] Hierarchy Level](#)
- [\[edit security resource-manager\] Hierarchy Level](#)
- [\[edit security screen\] Hierarchy Level](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level](#)
- [\[edit security traceoptions\] Hierarchy Level](#)
- [\[edit security utm\] Hierarchy Level](#)
- [\[edit security zones\] Hierarchy Level](#)

#### **Related Documentation**

- [Layer 2 Bridging and Switching Feature Guide for Security Devices](#)
- [Ethernet Port Switching Feature Guide for Security Devices](#)
- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)
- [Layer 2 Bridging and Switching Feature Guide for Security Devices](#)



[\[edit security alarms\] Hierarchy Level](#)

```

security {
 alarms {
 audible {
 continuous;
 }
 potential-violation {
 authentication failures;
 cryptographic-self-test;
 decryption-failures {
 threshold value;
 }
 encryption-failures {
 threshold value;
 }
 idp;
 ike-phase1-failures {
 threshold value;
 }
 ike-phase2-failures {
 threshold value;
 }
 key-generation-self-test;
 non-cryptographic-self-test;
 policy {
 application {
 duration interval;
 size count;
 threshold value;
 }
 destination-ip {
 duration interval;
 size count;
 threshold value;
 }
 policy match {
 duration interval;
 size count;
 threshold value;
 }
 source-ip {
 duration interval;
 size count;
 threshold value;
 }
 }
 replay-attacks {
 threshold value;
 }
 security-log-percent-full percentage;
 }
 }
}

```

**Related Documentation** • [Security Configuration Statement Hierarchy on page 57](#)

### [\[edit security datapath-debug\] Hierarchy Level](#)

```
security {
 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 files-number;
 format pacp-format;
 (no-world-readable | world-readable);
 size maximum-file-size;
 }
 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;
 }
 trace-options {
 file {
 filename;
 files files-number;
 match regular-expression;
 (no-world-readable | world-readable);
 size maximum-file-size;
 }
 no-remote-trace;
 }
 }
}
```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)
  - [Understanding Logical Systems for SRX Series Services Gateways](#)

#### [\[edit security traceoptions\] Hierarchy Level](#)

```
security {
 traceoptions {
 file {
 filename;
 files number;
 match regular-expression;
 (no-world-readable | world-readable);
 size maximum-file-size;
 }
 flag flag;
 no-remote-trace;
 rate-limit messages-per-second;
 }
}
```

- Related Documentation**
- [Security Configuration Statement Hierarchy on page 57](#)

### [accounting-options](#)

<b>Syntax</b>	accounting-options {...} }
<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. 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></li> <li>• <a href="#">Accounting Options Configuration on page 1289</a></li> </ul>

## 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 1518](#)

---

## archive-sites

---

**Syntax** archive-sites {  
    *site-name*;  
}

**Hierarchy Level** [edit accounting-options [file](#) *filename*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** 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 *router-name\_log-filename\_timestamp*.

**Options** *site-name*—Any valid FTP URL to a destination.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Archive Sites on page 1294](#)

## capture-file (Security)

---

<b>Syntax</b>	<pre>capture-file {     filename;     files number;     format <i>pcap-format</i>;     size <i>maximum-file-size</i>;     (world-readable   no-world-readable); }</pre>
<b>Hierarchy Level</b>	[edit security datapath-debug]
<b>Release Information</b>	Statement introduced in Release 10.4 of Junos OS.
<b>Description</b>	Sets packet capture for performing the datapath-debug action.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>filename</b>—Name of the file to receive the output of the packet capturing operation.</li><li>• <b>files</b>—Maximum number of capture files.  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.  Range: 1 through 10 files</li><li>• <b>format</b>—Describes the format of the capture file. The default format file is pcap. You can also set it as private (binary) format.</li><li>• <b>size</b>—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 <b>files</b> option and a filename.  Range: 10 KB through 100 MB</li><li>• <b>world-readable   no-world-readable</b>—By default, log files can be accessed only by the user who configures the tracing operation. The <b>world-readable</b> option enables any user to read the file. To explicitly set the default behavior, use the <b>no-world-readable</b> option.</li></ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. 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>

## class-usage-profile

Syntax	<pre> class-usage-profile <i>profile-name</i> {   file <i>filename</i>;   interval <i>minutes</i>;   source-classes {     source-class-name;   }   destination-classes {     destination-class-name;   } } </pre>
Hierarchy Level	[edit accounting-options]
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>
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	<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"> <li><a href="#">Configuring Class Usage Profiles on page 1304</a></li> </ul>

## cluster (Chassis)

```

Syntax cluster {
 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. 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 1581</a></li></ul>

---

## counters

---

<b>Syntax</b>	<pre>counters {   counter-name; }</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. 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. 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 1298</a></li></ul>

## 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.

<b>Description</b>	Configure the data path debugging options.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Security Configuration Statement Hierarchy on page 57</a></li> <li>• <a href="#">Understanding Data Path Debugging for Logical Systems</a></li> <li>• <a href="#">Packet Capture Overview on page 1508</a></li> <li>• <a href="#">Understanding Data Path Debugging for SRX Series Devices on page 1477</a></li> </ul>

## decryption-failures

---

<b>Syntax</b>	decryption-failures { threshold <i>value</i> ; }
<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>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Dynamic VPN Overview</a></li> <li>• <a href="#">Group VPN Overview</a></li> <li>• <a href="#">IPsec VPN Overview</a></li> </ul>

## destination-classes

---

<b>Syntax</b>	<code>destination-classes {     <i>destination-class-name</i>; }</code>
<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. 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>	<b><i>destination-class-name</i></b> —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. 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 1305</a></li></ul>

## destination-interface

Syntax	<code>destination-interface <i>interface-name</i>;</code>
Hierarchy Level	[edit services ( rpm probe owner test <i>test-name</i> ), [edit services rpm probe-server (tcp   udp)]]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	<p>On M Series and T Series routers, specify a services (<b>sp-</b>) interface that adds a timestamp to RPM probe messages. This feature is supported only with <b>icmp-ping</b>, <b>icmp-ping-timestamp</b>, <b>udp-ping</b>, and <b>udp-ping-timestamp</b> probe types. You must also configure the <b>rpm</b> statement on the <b>sp-</b> interface and include the <b>unit 0 family inet</b> statement with a <b>/32</b> address.</p> <p>On M Series, MX Series, and T Series routers, specify a multiservices (<b>ms-</b>) interface that adds a timestamp to RPM probe messages. This feature is supported only with <b>icmp-ping</b>, <b>icmp-ping-timestamp</b>, <b>udp-ping</b>, and <b>udp-ping-timestamp</b> probe types. You must also configure the <b>rpm</b> statement on the <b>ms-</b> interface and include the <b>unit 0 family inet</b> statement with a <b>/32</b> address.</p> <p>To enable RPM for the Services SDK on the adaptive services interface, configure the <b>object-cache-size</b>, <b>policy-db-size</b>, and <b>package</b> statements at the [edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package extension-provider] hierarchy level. For the Services SDK, <i>package-name</i> in the <b>package <i>package-name</i></b> statement is <b>jservices-rpm</b>.</p>
Options	<i>interface-name</i> —Name of the adaptive services interface.
Required Privilege Level	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <li>• <a href="#">hardware-timestamp on page 1577</a></li> </ul>

## destination-port

---

<b>Syntax</b>	<code>destination-port <i>port</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit services rpm probe <i>owner</i> test <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port to which a probe is sent. This statement is used only for TCP or UDP probe types.
<b>Options</b>	<i>port</i> —The port number can be 7 or from 49,160 through 65,535.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## fields (for Interface Profiles)

<b>Syntax</b>	fields { <i>field-name</i> ; }
<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. 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>	<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 1295</a></li> </ul>

## fields (for Routing Engine Profiles)

---

<b>Syntax</b>	<pre>fields {     <i>field-name</i>; }</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 1308</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> ], [edit accounting-options <a href="#">filter-profile <i>profile-name</i></a> ], [edit accounting-options <a href="#">interface-profile <i>profile-name</i></a> ], [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ], [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. The [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ] hierarchy added in Junos OS Release 8.2. 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. 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 1295</a></li> <li>• <a href="#">Configuring the Filter Profile on page 1297</a></li> <li>• <a href="#">Configuring the MIB Profile on page 1307</a></li> <li>• <a href="#">Configuring the Routing Engine Profile on page 1308</a></li> </ul>

## file (Configuring a Log File)

---

<b>Syntax</b>	<pre>file <i>filename</i> {     archive-sites {         <i>site-name</i>;     }     files <i>number</i>;     nonpersistent;     size <i>bytes</i>;     source-classes <i>time</i>;     transfer-interval <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. 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 1292</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. 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. 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 1292</a></li> </ul>

## filter-profile

<b>Syntax</b>	<pre>filter-profile <i>profile-name</i> {     counters {         counter-name;     }     file <i>filename</i>;     interval <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	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.
<b>Options</b>	<i>profile-name</i> —Name of the filter profile.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Filter Profile on page 1297</a></li> </ul>

## flow (Security Flow)

```

Syntax flow {
 aging {
 early-ageout seconds;
 high-watermark percent;
 low-watermark percent;
 }
 allow-dns-reply;
 bridge {
 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;
}

```

<b>Hierarchy Level</b>	[edit security]
<b>Release Information</b>	Statement modified in Release 9.5 of Junos OS.
<b>Description</b>	<p>Determine how the device manages packet flow. The device can regulate packet flow in the following ways:</p> <ul style="list-style-type: none"> <li>• Enable or disable DNS replies when there is no matching DNS request.</li> <li>• Set the initial session-timeout values.</li> </ul>
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<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>• <i>Juniper Networks Devices Processing Overview</i></li> <li>• <i>Understanding Session Characteristics for SRX Series Services Gateways</i></li> <li>• <i>Understanding Flow in Logical Systems for SRX Series Devices</i></li> </ul>

## global-threshold

---

<b>Syntax</b>	<code>global-threshold <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>	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>	<b><i>number</i></b> —Value at which the IP monitoring weight will be applied against the redundancy group failover threshold. <b>Range:</b> 0 through 255 <b>Default:</b> 0
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1581</a></li></ul>

## global-weight

<b>Syntax</b>	<code>global-weight <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit chassis cluster redundancy-group <i>group-number</i> ip-monitoring ]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	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.
<b>Options</b>	<p><b><i>number</i></b> —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 1581</a></li> </ul>

## hardware-timestamp

<b>Syntax</b>	<code>hardware-timestamp;</code>
<b>Hierarchy Level</b>	<code>[edit services rpm probe <i>owner</i> test <i>test-name</i>]</code>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.1.</p> <p>Statement applied to MX Series routers in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p>
<b>Description</b>	Enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor. This feature is supported only with <b>icmp-ping</b> , <b>icmp-ping-timestamp</b> , <b>udp-ping</b> , and <b>udp-ping-timestamp</b> probe types.
<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>

## icmp

---

<b>Syntax</b>	icmp{ <code>destination-interface</code> <i>interface-name</i> ; }
<b>Hierarchy Level</b>	[edit services rpm <code>probe-server</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the port information for the ICMP server.  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. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Understanding ICMP Fragment Protection</i></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. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Security Configuration Statement Hierarchy on page 57</a></li></ul>



---

## interface-profile

---

<b>Syntax</b>	<pre>interface-profile <i>profile-name</i> {     <b>fields</b> {         <i>field-name</i>;     }     <b>file</b> <i>filename</i>;     <b>interval</b> <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	interface—To view this statement in the configuration. 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 1295</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> ], [edit accounting-options <a href="#">filter-profile <i>profile-name</i></a> ], [edit accounting-options <a href="#">interface-profile <i>profile-name</i></a> ], [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ], [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. The [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ] hierarchy level added in Junos OS Release 8.2. 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. <b>Range:</b> 1 through 2880 minutes <b>Default:</b> 30 minutes
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1295</a></li><li>• <a href="#">Configuring the Filter Profile on page 1297</a></li><li>• <a href="#">Configuring the MIB Profile on page 1307</a></li><li>• <a href="#">Configuring the Routing Engine Profile on page 1308</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** *family-name IP 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**

- [global-threshold on page 1576](#)
- [global-weight on page 1577](#)

## 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.

<b>Description</b>	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 • [rpm \(Services\) on page 1596](#)

## maximum-capture-size (Datapath Debug)

<b>Syntax</b>	<code>maximum-capture-size <i>maximum-capture-size</i>;</code>
<b>Hierarchy Level</b>	[edit security datapath-debug]
<b>Release Information</b>	Statement introduced in Release 10.0 of Junos OS.
<b>Description</b>	Specifies maximum packet capture length.
<b>Options</b>	<ul style="list-style-type: none"> <li><code>maximum-capture-size <i>maximum-capture-size</i></code>—Specify the maximum packet capture length.</li> </ul> <p><b>Range:</b> 68 through 10,000 bytes</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. 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>

## mib-profile

<b>Syntax</b>	<pre>mib-profile <i>profile-name</i> {   file <i>filename</i>;   interval <i>minutes</i>;   object-names {     <i>mib-object-name</i>;   }   operation <i>operation-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Create a MIB profile to collect selected MIB statistics and write them to a file in the <code>/var/log</code> directory.
<b>Options</b>	<p><b><i>profile-name</i></b>—Name of the MIB statistics profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1307</a></li> </ul>

## mpls (Security Forwarding Options)

---

<b>Syntax</b>	<code>mpls {     mode packet-based; }</code>
<b>Hierarchy Level</b>	[edit security forwarding-options family]
<b>Release Information</b>	Statement introduced in Release 9.0 of Junos OS.
<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: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.


<b>Required Privilege Level</b>	security—To view this statement in the configuration. 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>

## next-hop

---

<b>Syntax</b>	<code>next-hop <i>next-hop</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm probe <i>owner</i> test <i>test-name</i> ]
<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. services-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">probe on page 1589</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>	 <p><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.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1293</a></li> </ul>

## object-names

<b>Syntax</b>	<pre>object-names {   mib-object-name; }</pre>
<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. 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>	<i>mib-object-name</i> —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. 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 1307</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. 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. <b>Default:</b> walk
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1307</a></li></ul>



## packet-capture

---

<b>Syntax</b>	<pre>packet-capture {   disable;   file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>bytes</i>&gt; &lt;world-readable   no-world-readable&gt;;   maximum-capture-size <i>number</i>; }</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 1508</a></li></ul>

## packet-filter

<b>Syntax</b>	<pre>packet-filter <i>packet-filter-name</i> {   action-profile (<i>profile-name</i>   default);   destination-port (<i>port-range</i>   <i>protocol-name</i>);   destination-prefix <i>destination-prefix</i>;   interface <i>logical-interface-name</i>;   protocol (<i>protocol-number</i>   <i>protocol-name</i>);   source-port (<i>port-range</i>   <i>protocol-name</i>);   source-prefix <i>source-prefix</i>; }</pre>
<b>Hierarchy Level</b>	[edit security datapath-debug]
<b>Release Information</b>	<p>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.</p> <p>Support for IPv6 filter for the <b>interface</b> option added in Junos OS Release 10.4.</p>
<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>	<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="#">Security Configuration Statement Hierarchy on page 57</a></li> </ul>

## probe

```
Syntax probe owner {
 test test-name {
 data-fill data;
 data-size size;
 destination-interface interface-name;
 destination-port port;
 dscp-code-point dscp-bits;
 hardware-timestamp;
 history-size size;
 moving-average-size number;
 next-hop next-hop;
 one-way-hardware-timestamp;
 probe-count count;
 probe-interval seconds;
 probe-type type;
 routing-instance instance-name;
 source-address address;
 target (url | address);
 test-interval interval;
 thresholds
 {
 egress-time microseconds;
 ingress-time microseconds;
 jitter-egress microseconds;
 jitter-ingress microseconds;
 jitter-rtt microseconds;
 rtt microseconds;
 std-dev-egress microseconds;
 std-dev-ingress microseconds;
 std-dev-rtt microseconds;
 successive-loss count;
 total-loss count;
 }
 traps [trap-names];
 }
 }
```

**Hierarchy Level** [edit services rpm]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description** Specify an owner name. The owner name combined with the test name represent a single RPM configuration instance.

**Options** *owner*—Specify an owner name up to 32 characters in length.  
  
The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## probe-interval

---

<b>Syntax</b>	<code>probe-interval <i>interval</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit services rpm probe <i>owner</i> test <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify the time to wait between sending packets, in seconds.
<b>Options</b>	<i>interval</i> —Number of seconds, from 1 through 255.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## probe-limit

---

<b>Syntax</b>	<code>probe-limit <i>limit</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify the maximum number of concurrent probes allowed.
<b>Options</b>	<i>limit</i> —A value from 1 through 500. <b>Default:</b> 100.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## probe-server

---

**Syntax**    `probe-server {  
              tcp {  
                  destination-interface interface-name;  
                  port number;  
              }  
              udp {  
                  destination-interface interface-name;  
                  port number;  
              }  
          }`

**Hierarchy Level**    [edit services rpm]

**Release Information**    Statement introduced before Junos OS Release 7.4.  
                              Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description**    Specify the server to act as a receiver for the probes.  
  
                      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.

## probe-type

---

<b>Syntax</b>	<code>probe-type type;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit services rpm probe <i>owner</i> test <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify the packet and protocol contents of a probe.
<b>Options</b>	<p><b>type</b>—Specify one of the following probe type values:</p> <ul style="list-style-type: none"><li>• <b>http-get</b>—(Not available at the [edit services rpm bgp] hierarchy level.) Sends a Hypertext Transfer Protocol (HTTP) get request to a target URL.</li><li>• <b>http-metadata-get</b>—(Not available at the [edit services rpm bgp] hierarchy level.) Sends an HTTP get request for metadata to a target URL.</li><li>• <b>icmp-ping</b>—Sends ICMP echo requests to a target address.</li><li>• <b>icmp-ping-timestamp</b>—Sends ICMP timestamp requests to a target address.</li><li>• <b>tcp-ping</b>—Sends TCP packets to a target.</li><li>• <b>udp-ping</b>—Sends UDP packets to a target.</li><li>• <b>udp-ping-timestamp</b>—Sends UDP timestamp requests to a target address.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-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 1581](#)

---

## 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 1581](#)



## routing-engine-profile

---

<b>Syntax</b>	<pre>routing-engine-profile <i>profile-name</i> {     <i>fields</i> {         <i>field-name</i>;     }     <i>file</i> <i>filename</i>;     <i>interval</i> <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options]
<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>	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>	<p><i>profile-name</i>—Name of the Routing Engine statistics 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 Routing Engine Profile on page 1308</a></li> </ul>

## rpm (Services)

```

Syntax rpm {
 bgp {
 data-fill data;
 data-size size;
 destination-port port;
 history-size size;
 logical-system logical-system-name <routing-instances routing-instance-name>;
 moving-average-size number-of-samples;
 probe-count count;
 probe-interval seconds;
 probe-type type;
 routing-instances {
 routing-instance-name;
 }
 test-interval seconds;
 }
 probe owner {
 test test-name {
 data-fill data;
 data-size size;
 destination-interface interface-name;
 destination-port port;
 dscp-code-point dscp-bits;
 hardware-timestamp;
 history-size size;
 moving-average-size number;
 next-hop next-hop;
 one-way-hardware-timestamp;
 probe-count count;
 probe-interval seconds;
 probe-type type;
 routing-instance instance-name;
 source-address address;
 target {
 address address;
 url url;
 }
 test-interval interval;
 thresholds {
 egress-time microseconds;
 ingress-time microseconds;
 jitter-egress microseconds;
 jitter-ingress microseconds;
 jitter-rtt microseconds;
 rtt microseconds;
 std-dev-egress microseconds;
 std-dev-ingress microseconds;
 std-dev-rtt microseconds;
 successive-loss count;
 total-loss count;
 }
 traps [trap-names];
 }
 }
 }

```

```

 }
 }
 probe-limit number;
 probe-server {
 icmp {
 destination-interface interface-name;
 }
 tcp {
 destination-interface interface-name;
 port port-number;
 }
 udp {
 destination-interface interface-name;
 port port-number;
 }
 }
}

```

<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure real-time performance monitoring (RPM) probes.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">icmp on page 1578</a></li> </ul>

## size

---

Syntax	<code>size bytes;</code>
Hierarchy Level	[edit accounting-options <a href="#">file</a> <i>filename</i> ]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify attributes of an accounting-data log file.
Options	<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.  <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 <b>Range:</b> 256 KB through 1 GB
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"><li>• <a href="#">Configuring the Maximum Size of the File on page 1293</a></li></ul>

## source-classes

---

Syntax	<pre>source-classes {     <i>source-class-name</i>; }</pre>
Hierarchy Level	[edit accounting-options <a href="#">class-usage-profile</a> <i>profile-name</i> ]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the source classes for which statistics are collected.
Options	<b>source-class-name</b> —Name of the source class to include in the class usage profile.
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"><li>• <a href="#">Configuring a Class Usage Profile on page 1305</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. 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. <b>Syntax:</b> <code>YYYY-MM-DD.hh:mm</code>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. 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 1293</a></li> </ul>

## target

---

<b>Syntax</b>	<code>target (url <i>url</i>   address <i>address</i>);</code>
<b>Hierarchy Level</b>	[edit services rpm probe <i>owner</i> test <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify the destination address used for the probes.
<b>Options</b>	<p><b>url <i>url</i></b>—For HTTP probe types, specify a fully formed URL that includes <b>http://</b> in the URL address.</p> <p><b>address <i>address</i></b>—For all other probe types, specify an IPv4 address for the target host.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## thresholds

---

<b>Syntax</b>	<code>thresholds thresholds;</code>
<b>Hierarchy Level</b>	<code>[edit services rpm probe owner test test-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Specify thresholds used for the probes. A system log message is generated when the configured threshold is exceeded. Likewise, an SNMP trap (if configured) is generated when a threshold is exceeded.
<b>Options</b>	<p><b>thresholds</b>—Specify one or more threshold measurements. The following options are supported:</p> <ul style="list-style-type: none"><li>• <b>egress-time</b>—Measures maximum source-to-destination time per probe.</li><li>• <b>ingress-time</b>—Measures maximum destination-to-source time per probe.</li><li>• <b>jitter-egress</b>—Measures maximum source-to-destination jitter per test.</li><li>• <b>jitter-ingress</b>—Measures maximum destination-to- source jitter per test.</li><li>• <b>jitter-rtt</b>—Measures maximum jitter per test, from 0 through 60,000,000 microseconds.</li><li>• <b>rtt</b>—Measures maximum round-trip time per probe, in microseconds.</li><li>• <b>std-dev-egress</b>—Measures maximum source-to-destination standard deviation per test.</li><li>• <b>std-dev-ingress</b>—Measures maximum destination-to-source standard deviation per test.</li><li>• <b>std-dev-rtt</b>—Measures maximum standard deviation per test, in microseconds.</li><li>• <b>successive-loss</b>—Measures successive probe loss count, indicating probe failure. Default: 1</li><li>• <b>total-loss</b>—Measures total probe loss count indicating test failure, from 0 through 15. Default: 1</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## 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 <b>/var/log</b>. 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.
- Required Privilege Level** trace—To view this statement in the configuration.  
trace-control—To add this statement to the configuration.
- Related Documentation** • [Security Configuration Statement Hierarchy on page 57](#)

---

## transfer-interval

---

- Syntax** transfer-interval *minutes*;
- Hierarchy Level** [edit accounting-options [file](#) *filename*]
- Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Description** Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.
- Options** *minutes*—Time the file remains open and receives new statistics before it is closed and transferred to an archive site.  
**Range:** 5 through 2880 minutes  
**Default:** 30 minutes
- Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.
- Related Documentation** • [Configuring the Transfer Interval of the File on page 1294](#)



## traps

<b>Syntax</b>	<code>traps traps;</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 before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Set the trap bit to generate traps for probes. Traps are sent if the configured threshold is met or exceeded.
<b>Options</b>	<p><b>traps</b>—Specify one or more traps. The following options are supported:</p> <ul style="list-style-type: none"> <li>• <b>egress-jitter-exceeded</b>—Generates traps when the jitter in egress time threshold is met or exceeded.</li> <li>• <b>egress-std-dev-exceeded</b>—Generates traps when the egress time standard deviation threshold is met or exceeded.</li> <li>• <b>egress-time-exceeded</b>—Generates traps when the maximum egress time threshold is met or exceeded.</li> <li>• <b>ingress-jitter-exceeded</b>—Generates traps when the jitter in ingress time threshold is met or exceeded.</li> <li>• <b>ingress-std-dev-exceeded</b>—Generates traps when the ingress time standard deviation threshold is met or exceeded.</li> <li>• <b>ingress-time-exceeded</b>—Generates traps when the maximum ingress time threshold is met or exceeded.</li> <li>• <b>jitter-exceeded</b>—Generates traps when the jitter in round-trip time threshold is met or exceeded.</li> <li>• <b>probe-failure</b>—Generates traps for successive probe loss thresholds crossed.</li> <li>• <b>rtt-exceeded</b>—Generates traps when the maximum round-trip time threshold is met or exceeded.</li> <li>• <b>std-dev-exceeded</b>—Generates traps when the round-trip time standard deviation threshold is met or exceeded.</li> <li>• <b>test-completion</b>—Generates traps when a test is completed.</li> <li>• <b>test-failure</b>—Generates traps when the total probe loss threshold is met or exceeded.</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>

## Operational Commands

- `clear chassis cluster ip-monitoring failure-count`
- `clear chassis cluster ip-monitoring failure-count ip-address`

- [monitor list](#)
- [monitor start](#)
- [monitor stop](#)
- [monitor traffic](#)
- [mtrace monitor](#)
- [ping mpls l2circuit](#)
- [ping mpls l2vpn](#)
- [ping mpls l3vpn](#)
- [ping mpls ldp](#)
- [ping mpls lsp-end-point](#)
- [ping mpls rsvp](#)
- [request pppoe connect](#)
- [request pppoe disconnect](#)
- [request services ip-monitoring preempt-restore policy](#)
- [show chassis alarms](#)
- [show configuration](#)
- [show chassis cluster ip-monitoring status redundancy-group](#)
- [show interfaces \(SRX Series\)](#)
- [show poe interface \(View\)](#)
- [show poe telemetries](#)
- [show pppoe interfaces](#)
- [show pppoe statistics](#)
- [show security alarms](#)
- [show security datapath-debug capture](#)
- [show security datapath-debug counter](#)
- [show security monitoring fpc fpc-number](#)
- [show security monitoring performance session](#)
- [show security monitoring performance spu](#)
- [show services ip-monitoring status](#)
- [show services rpm probe-results \(View\)](#)
- [show system alarms](#)
- [traceroute](#)

## 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>• <i>clear chassis cluster failover-count</i></li><li>• <a href="#">clear chassis cluster ip-monitoring failure-count ip-address on page 1606</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 1605</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

```

## monitor list

<b>Syntax</b>	monitor list
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display the status of monitored log and trace files.
<b>Options</b>	This command has no options.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">monitor start on page 1608</a></li> <li>• <a href="#">monitor stop on page 1610</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor list on page 1607</a>
<b>Output Fields</b>	<a href="#">Table 225 on page 1607</a> describes the output fields for the <b>monitor list</b> command. Output fields are listed in the approximate order in which they appear.

**Table 225: monitor list Output Fields**

Field Name	Field Description
<b>monitor start</b>	Indicates the file is being monitored.
<b>"filename"</b>	Name of the file that is being monitored.
<b>Last changed</b>	Date and time at which the file was last modified.

## Sample Output

### monitor list

```
user@host> monitor list
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)
```

## monitor start

<b>Syntax</b>	<code>monitor start <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Start displaying the system log or trace file and additional entries being added to those files.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.



**NOTE:** To monitor a log file within a logical system, issue the `monitor start logical-system-name/filename` command.

<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">monitor list on page 1607</a></li> <li><a href="#">monitor stop on page 1610</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor start on page 1609</a>
<b>Output Fields</b>	<a href="#">Table 226 on page 1608</a> describes the output fields for the <b>monitor start</b> command. Output fields are listed in the approximate order in which they appear.

**Table 226: monitor start Output Fields**

Field Name	Field Description
<b>***<i>filename</i>***</b>	Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.
<b><i>Date and time</i></b>	Timestamp for the log entry.

## Sample Output

### monitor start

```
user@host> monitor start system-log
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: RSA key generation complete.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: RSA authentication for root accepted.
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from host.example.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
```

## monitor stop

---

<b>Syntax</b>	<code>monitor stop <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Stop displaying the system log or trace file.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols <i>protocol</i>]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">monitor list on page 1607</a></li><li>• <a href="#">monitor start on page 1608</a></li></ul>
<b>List of Sample Output</b>	<a href="#">monitor stop on page 1610</a>
<b>Output Fields</b>	This command produces no output.

## Sample Output

### monitor stop

```
user@host> monitor stop
```



## monitor traffic

**Syntax** monitor traffic  
 <brief | detail | extensive>  
 <absolute-sequence>  
 <count *count*>  
 <interface *interface-name*>  
 <layer2-headers>  
 <matching *matching*>  
 <no-domain-names>  
 <no-promiscuous>  
 <no-resolve>  
 <no-timestamp>  
 <print-ascii>  
 <print-hex>  
 <resolve-timeout>  
 <size *size*>

**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.

**Description** Display packet headers or packets received and sent from the Routing Engine.



### NOTE:

- Using the **monitor-traffic** command can degrade router or switch performance.
- Delays from DNS resolution can be eliminated by using the **no-resolve** option.



**NOTE:** This command is not supported on the QFX3000 QFabric switch.

**Options** **none**—(Optional) Display packet headers transmitted through **fxp0**. On a TX Matrix Plus router, display packet headers transmitted through **em0**.



**NOTE:** On SRX3400 and SRX3600 devices, when you enable the monitor traffic option using the monitor traffic command to monitor the FXP interface traffic, interface bounce occurs. You must use the monitor traffic interface fxp0 no-promiscuous command to avoid the issue.

**brief | detail | extensive**—(Optional) Display the specified level of output.

**absolute-sequence**—(Optional) Display absolute TCP sequence numbers.

**count *count***—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The **monitor traffic** command quits automatically after displaying the number of packets specified.

**interface *interface-name***—(Optional) Specify the interface on which the **monitor traffic** command displays packet data. If no interface is specified, the **monitor traffic** command displays packet data arriving on the lowest-numbered interface.

**layer2-headers**—(Optional) Display the link-level header on each line.

**matching *matching***—(Optional) Display packet headers that match a regular expression. Use matching expressions to define the level of detail with which the **monitor traffic** command filters and displays packet data.

**no-domain-names**—(Optional) Suppress the display of the domain portion of hostnames. With the **no-domain-names** option enabled, the **monitor traffic** command displays only **team** for the hostname **host.example.com**.

**no-promiscuous**—(Optional) Do not put the interface into promiscuous mode.

**no-resolve**—(Optional) Suppress reverse lookup of the IP addresses.

**no-timestamp**—(Optional) Suppress timestamps on displayed packets.

**print-ascii**—(Optional) Display each packet in ASCII format.

**print-hex**—(Optional) Display each packet, except the link-level header, in hexadecimal format.

**resolve-timeout *timeout***—(Optional) Amount of time the router or switch waits for each reverse lookup before timing out. You can set the timeout for 1 through 4,294,967,295 seconds. The default is 4 seconds. To display each packet, use the **print-ascii**, **print-hex**, or **extensive** option.

**size *size***—(Optional) Read but do not display up to the specified number of bytes for each packet. When set to **brief** output, the default packet size is 96 bytes and is adequate for capturing IP, ICMP, UDP, and TCP packet data. When set to **detail** and **extensive** output, the default packet size is 1514. The **monitor traffic** command truncates displayed packets if the matched data exceeds the configured size.

**Additional Information** In the **monitor traffic** command, you can specify an expression to match by using the **matching** option and including the expression in quotation marks:

**monitor traffic matching "*expression*"**

Replace ***expression*** with one or more of the match conditions listed in [Table 227 on page 1613](#).

Table 227: Match Conditions for the monitor traffic Command

Match Type	Condition	Description
Entity	<b>host</b> [ <i>address</i>   <i>hostname</i> ]	Matches packets that contain the specified address or hostname.  The protocol match conditions <b>arp</b> , <b>ip</b> , or <b>rarp</b> , or any of the directional match conditions can be prepended to the <b>host</b> match condition.
	<b>net</b> <i>address</i>	Matches packets with source or destination addresses containing the specified network address.
	<b>net</b> <i>address mask mask</i>	Matches packets containing the specified network address and subnet mask.
	<b>port</b> ( <i>port-number</i>   <i>port-name</i> )	Matches packets containing the specified source or destination TCP or UDP port number or port name.  In place of the numeric port address, you can specify a text synonym, such as <b>bgp</b> (179), <b>dhcp</b> (67), or <b>domain</b> (53) (the port numbers are also listed).
Directional	<b>dst</b>	Matches packets going to the specified destination. This match condition can be prepended to any of the entity type match conditions.
	<b>src</b>	Matches packets from a specified source. This match condition can be prepended to any of the entity type match conditions.
	<b>src and dst</b>	Matches packets that contain the specified source and destination addresses. This match condition can be prepended to any of the entity type match conditions.
	<b>src or dst</b>	Matches packets containing either of the specified addresses. This match condition can be prepended to any of the entity type match conditions.
Packet Length	<b>less</b> <i>value</i>	Matches packets shorter than or equal to the specified value, in bytes.
	<b>greater</b> <i>value</i>	Matches packets longer than or equal to the specified value, in bytes.

Table 227: Match Conditions for the monitor traffic Command (*continued*)

Match Type	Condition	Description
Protocol	<b>amt</b>	Matches all AMT packets. Use the extensive level of output to decode the inner IGMP packets in addition to the AMT outer packet.
	<b>arp</b>	Matches all ARP packets.
	<b>ether</b>	Matches all Ethernet packets.
	<b>ether (broadcast   multicast)</b>	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with <b>src</b> and <b>dst</b> .
	<b>ether protocol (address   (arp   ip   rarp))</b>	Matches packets with the specified Ethernet address or Ethernet packets of the specified protocol type. The <b>ether protocol</b> arguments <b>arp</b> , <b>ip</b> , and <b>rarp</b> are also independent match conditions, so they must be preceded by 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 (broadcast   multicast)</b>	Matches broadcast or multicast IP packets.
	<b>ip protocol (address   (icmp   igmp   tcp   udp))</b>	Matches packets with the specified address or protocol type. The <b>ip protocol</b> arguments <b>icmp</b> , <b>tcp</b> , and <b>udp</b> are also independent match conditions, so they must be preceded by 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 datagrams.
	<b>udp</b>	Matches all UDP datagrams.

To combine expressions, use the logical operators listed in [Table 228 on page 1614](#).

Table 228: Logical Operators for the monitor traffic Command

Logical Operator (Highest to Lowest Precedence)	Description
<b>!</b>	Logical NOT. If the first condition does not match, the next condition is evaluated.

Table 228: Logical Operators for the monitor traffic Command (*continued*)

Logical Operator (Highest to Lowest Precedence)	Description
&&	Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.
	Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.
()	Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).

You can use relational operators to compare arithmetic expressions composed of integer constants, binary operators, a length operator, and special packet data accessors. The arithmetic expression matching condition uses the following syntax:

```
monitor traffic matching "ether[0] & 1 != 0"arithmetic_expression relational_operator arithmetic_expression
```

The packet data accessor uses the following syntax:

```
protocol [byte-offset <size>]
```

The optional *size* field represents the number of bytes examined in the packet header. The available values are 1, 2, or 4 bytes. The following sample command captures all multicast traffic:

```
user@host> monitor traffic matching "ether[0] & 1 != 0"
```

To specify match conditions that have a numeric value, use the arithmetic and relational operators listed in [Table 229 on page 1616](#).



**NOTE:** Because the Packet Forwarding Engine removes Layer 2 header information before sending packets to the Routing Engine:

- The **monitor traffic** command cannot apply match conditions to inbound traffic.
- The **monitor traffic interface** command also cannot apply match conditions for Layer 3 and Layer 4 packet data, resulting in the match pipe option (`| match`) for this command for Layer 3 and Layer 4 packets not working either. Therefore, ensure that you specify match conditions as described in this command summary. For more information about match conditions, see [Table 227 on page 1613](#).
- The 802.1Q VLAN tag information included in the Layer 2 header is removed from all inbound traffic packets. Because the **monitor traffic interface ae[x]** command for aggregated Ethernet interfaces (such as ae0) only shows inbound traffic data, the command does not show VLAN tag information in the output.

**Table 229: Arithmetic and Relational Operators for the monitor traffic Command**

Arithmetic or Relational Operator	Description
<b>Arithmetic Operator</b>	
+	Addition operator.
-	Subtraction operator.
/	Division operator.
&	Bitwise AND.
*	Bitwise exclusive OR.
	Bitwise inclusive OR.
<b>Relational Operator (Highest to Lowest Precedence)</b>	
<=	If the first expression is less than or equal to the second, the packet matches.
>=	If the first expression is greater than or equal to the second, the packet matches.
<	If the first expression is less than the second, the packet matches.
>	If the first expression is greater than the second, the packet matches.
=	If the compared expressions are equal, the packet matches.
!=	If the compared expressions are unequal, the packet matches.

**Required Privilege Level** trace  
maintenance

**List of Sample Output** [monitor traffic count on page 1617](#)  
[monitor traffic detail count on page 1617](#)  
[monitor traffic extensive \(Absolute Sequence\) on page 1617](#)  
[monitor traffic extensive \(Relative Sequence\) on page 1617](#)  
[monitor traffic extensive count on page 1617](#)  
[monitor traffic interface on page 1618](#)  
[monitor traffic matching on page 1618](#)  
[monitor traffic \(TX Matrix Plus Router\) on page 1618](#)  
[monitor traffic \(QFX3500 Switch\) on page 1619](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### monitor traffic count

```
user@host> monitor traffic count 2
listening on fxp0
04:35:49.814125 In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529478 win 16798 (DF)
04:35:49.814185
Out my-server.work.net.telnet > my-server.home.net.1295: P
1:38(37) ack 0 win 17680 (DF) [tos 0x10]
```

### monitor traffic detail count

```
user@host> monitor traffic detail count 2
listening on fxp0
04:38:16.265864 In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529971 win 17678 (DF) (ttl 121, id 6812)
04:38:16.265926
Out my-server.work.net.telnet.telnet > my-server.home.net.1295: P 1:38(37) ack 0
win 17680 (DF) [tos 0x10] (ttl 6)
```

### monitor traffic extensive (Absolute Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp" absolute-sequence
listening on fxp0
In 207.17.136.193.179 > 192.168.4.227.1024: . 4042780859:4042780859(0)
ack 1845421797 win 16384 <nop,nop,timestamp 4935628 965951> [tos 0xc0] (ttl)
In 207.17.136.193.179 > 192.168.4.227.1024: P 4042780859:4042780912(53)
ack 1845421797 win 16384
<nop,nop,timestamp 4935628 965951>:
BGP [|BGP UPDAT)
In 192.168.4.227.1024 > 207.17.136.193.179:
P 1845421797:1845421852(55) ack 4042780912 win 16384 <nop,nop,timestamp 965951
4935628>: BGP [|BGP UPDAT)
...
```

### monitor traffic extensive (Relative Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp"
listening on fxp0
In 172.24.248.221.1680 > 192.168.4.210.23: . 396159737:396159737(0)
ack 1664980689 win 17574 (DF) (ttl 121, id 50003)
Out 192.168.4.210.23 > 172.24.248.221.1680: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10] (ttl 64, id 5394)
In 207.17.136.193.179 > 192.168.4.227.1024: P 4042775817:4042775874(57)
ack 1845416593 win 16384 <nop,nop,timestamp 4935379 965690>: BGP [|BGP UPDAT)
...
```

### monitor traffic extensive count

```
user@host> monitor traffic extensive count 5 no-domain-names no-resolve
listening on fxp013:18:17.406933
In 192.168.4.206.2723610880 > 172.17.28.8.2049:
40 null (ttl 64, id 38367)13:18:17.407577
In 172.17.28.8.2049 > 192.168.4.206.2723610880:
```

```

reply ok 28 null (ttl 61, id 35495)13:18:17.541140
In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
0000 0100 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 000013:18:17.591513
In 172.24.248.156.4139 > 192.168.4.210.23:
3556964918:3556964918(0)
ack 295526518 win 17601 (DF)
(ttl 121, id 14)13:18:17.591568
Out 192.168.4.210.23 >
172.24.248.156.4139: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]
(ttl 64, id 52376)

```

### monitor traffic interface

```

user@host> monitor traffic interface fxp0
listening on fxp0.0
18:17:28.800650 In server.home.net.723 > host1-0.lab.home.net.log
18:17:28.800733 Out host2-0.lab.home.net.login > server.home.net.7
18:17:28.817813 In host30.lab.home.net.syslog > host40.home0
18:17:28.817846 In host30.lab.home.net.syslog > host40.home0
...

```

### monitor traffic matching

```

user@host> monitor traffic matching "net 192.168.1.0/24"
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes

Reverse lookup for 192.168.1.255 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use no-resolve to avoid reverse lookups on IP addresses.

21:55:54.003511 In IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003585 Out IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003864 In arp who-has 192.168.1.17 tell 192.168.1.9
...

```

### monitor traffic (TX Matrix Plus Router)

```

user@host> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em0, capture size 96 bytes
04:11:59.862121 Out IP truncated-ip - 25 bytes missing!
host1.example.com.syslog > host2.example.com.syslog:
SYSLOG kernel.info, length: 57
04:11:59.862303
Out IP truncated-ip - 25 bytes missing!
host1.example.com.syslog >
host3.example.com.syslog: SYSLOG kernel.info, length: 57
04:11:59.923948
In IP host4.example.com.65235 >

```



```

host1.example.com.telnet: .
ack 1087492766 win 33304 <nop,nop,timestamp 42366734 993490>
04:11:59.923983 Out IP truncated-ip - 232 bytes missing!
host1.example.com.telnet > host4.example.com.65235: P 1:241(240) ack 0 win 33304

<nop,nop,timestamp 993590 42366734>
04:12:00.022900
In IP host4.example.com.65235 >
host1.example.com.telnet: . ack 241 win 33304 <nop,nop,timestamp 42366834 993590>
04:12:00.141204
In IP truncated-ip - 40 bytes missing!
host5.example.com.46182 > host1.example.com.telnet: P 2950530356:2950530404(48)
ack 485494987 win 63712
<nop,nop,timestamp 1308555294 987086>
04:12:00.141345
Out IP host1.example.com.telnet >
host5.example.com.46182: P 1:6(5)
ack 48 win 33304
<nop,nop,timestamp 993809 1308555294>
04:12:00.141572
In IP host5.example.com.46182 >
host1.example.com.telnet: .
ack 6 win 63712
<nop,nop,timestamp 1308555294 993809>
04:12:00.141597
Out IP host1.example.com.telnet >
host5.example.com.46182: P 6:10(4) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.141821
In IP host5.example.com.46182 >
host1.example.com.telnet: .
ack 10 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.141837 Out IP truncated-ip - 2 bytes missing!
host1.example.com.telnet >
host5.example.com.46182: P 10:20(10) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.142072
In IP host5.example.com.46182 >
host1.example.com.telnet: . ack 20 win 63712
<nop,nop,timestamp 1308555294 993810>
04:12:00.142089 Out IP host1.example.com.telnet >
host5.example.com.46182: P 20:28(8) ack 48 win 33304 <nop,nop,timestamp 993810
1308555294>
04:12:00.142321
In IP host5.example.com.46182 >
host1.example.com.telnet: .
ack 28 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.142337
Out IP truncated-ip - 1 bytes missing!
host1.example.com.telnet >
host5.example.com.46182: P 28:37(9) ack 48 win 33304 <nop,nop,timestamp 993810
1308555294>
...

```

### monitor traffic (QFX3500 Switch)

```

user@switch> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on me4, capture size 96 bytes

```

```
Reverse lookup for 172.22.16.246 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.
16:35:32.240873 Out IP truncated-ip - 112 bytes missing! host6.example.com.ssh >

172.22.16.246.telefinder: P 4200727624:4200727756(132) ack 2889954831 win 65535
16:35:32.240900 Out IP truncated-ip - 176 bytes missing! host6.example.com.ssh >

172.22.16.246.telefinder: P 132:328(196) ack 1 win 65535
...
```

## mtrace monitor

<b>Syntax</b>	mtrace monitor
<b>Release Information</b>	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 11.3 for the QFX Series.
<b>Description</b>	Listen passively for IP multicast responses. To exit the <b>mtrace monitor</b> command, type Ctrl+c.
<b>Options</b>	<b>none</b> —Trace the master instance.
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">mtrace monitor on page 1622</a>
<b>Output Fields</b>	<a href="#">Table 230 on page 1621</a> describes the output fields for the <b>mtrace monitor</b> command. Output fields are listed in the approximate order in which they appear.

**Table 230: mtrace monitor Output Fields**

Field Name	Field Description
<b>Mtrace query at</b>	Date and time of the query.
<b>by</b>	Address of the host issuing the query.
<b>resp to</b>	Response destination.
<b>qid</b>	Query ID number.
<b>packet from...to</b>	IP address of the query source and default group destination.
<b>from...to</b>	IP address of the multicast source and the response address.
<b>via group</b>	IP address of the group to trace.
<b>mxhop</b>	Maximum hop setting.

## Sample Output

### mtrace monitor

```
user@host> mtrace monitor
Mtrace query at Oct 22 13:36:14 by 192.1.3.2, resp to 224.0.1.32, qid 74a5b8
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:17 by 192.1.3.2, resp to 224.0.1.32, qid 1d07ba
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:20 by 192.1.3.2, resp to same, qid 2fea1d
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:30 by 192.1.3.2, resp to same, qid 7c88ad
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)
```

## ping mpls l2circuit

**Syntax** ping mpls l2circuit (interface *interface-name* | virtual-circuit *virtual-circuit-id* neighbor *address*)  
 <count *count*>  
 <destination *address*>  
 <detail>  
 <exp *forwarding-class*>  
 <logical-system (all | *logical-system-name*)>  
 reply-mode (application-level-control-channel | ip-udp | no-reply)  
 <size *bytes*>  
 <source *source-address*>  
 <sweep>  
 <v1>

**Release Information** Command introduced before Junos OS Release 7.4.  
 Command introduced in Junos OS Release 9.0 for EX Series switches.  
 Statement introduced in Junos OS Release 12.3X50 for the QFX Series.  
 The **size** and **sweep** options were introduced in Junos OS Release 9.6.  
 The **reply-mode** option and its suboptions are introduced in Junos OS Release 10.4R1.

**Description** Check the operability of the MPLS Layer 2 circuit connections. Type Ctrl+c to interrupt a ping mpls l2circuit command.

**Options** **count** *count*—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.

**destination** *address*—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.

**detail**—(Optional) Display detailed information about the echo requests sent and received.

**exp** *forwarding-class*—(Optional) Value of the forwarding class for the MPLS ping packets.

**interface** *interface-name*—Ping an interface configured for the Layer 2 circuit on the egress provider edge (PE) router.

**logical-system** (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on the specified logical system.

**reply-mode**—(Optional) Reply mode for the ping request. This option has the following suboptions:

**application-level-control-channel**—Reply using an application level control channel.

**ip-udp**—Reply using an IPv4 or IPv6 UDP packet.

**no-reply**—Do not reply to the ping request.



**NOTE:** The **reply-mode** option and its suboptions **application-level-control-channel**, **ip-udp**, and **no-reply** are also available in Junos OS Release 10.2R4 and 10.3R2.

**size bytes**—(Optional) Size of the label-switched path (LSP) ping request packet (96 through 65468 bytes). Packets are 4-byte aligned. For example, If you enter a size of 97, 98, 99, or 100, the router or switch uses a size value of 100 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 96-byte minimum.

**source source-address**—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**vl**—(Optional) Use the type 9 Layer 2 circuit type, length, and value (TLV).

**virtual-circuit virtual-circuit-id neighbor address**—Ping the virtual circuit identifier on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.

**Additional Information** You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the egress PE router or switch (the router or switch receiving the MPLS echo packets) to ping a Layer 2 circuit.

In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

**Required Privilege Level** network

**List of Sample Output** [ping mpls l2circuit interface on page 1625](#)  
[ping mpls l2circuit virtual-circuit detail on page 1625](#)  
[ping mpls l2circuit interface <interface-name> reply-mode on page 1625](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with an error code are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls l2circuit interface

```
user@host> ping mpls l2circuit interface so-1/0/0.1
Request for seq 1, to interface 69, labels <100000, 100208>, packet size 100
Reply for seq 1, return code: Egress-ok, time: 0.439 ms
```

### ping mpls l2circuit virtual-circuit detail

```
user@host> ping mpls l2circuit virtual-circuit 200 neighbor 10.255.245.122/32 detail
Request for seq 1, to interface 68, labels <100048, 100128>, packet size 100

Reply for seq 1, return code: Egress-ok time: 0.539 ms
```

### ping mpls l2circuit interface <interface-name> reply-mode

```
user@host> ping mpls l2circuit interface lt-1/2/0.21 reply-mode application-level-control-channel
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping mpls l2vpn

<b>Syntax</b>	<p>ping mpls l2vpn (instance <i>instance-name</i> local-site-id <i>local-site-id-number</i> remote-site-id <i>remote-site-id-number</i>   interface <i>interface-name</i>)</p> <p>&lt;bottom-label-ttl&gt;</p> <p>&lt;count <i>count</i>&gt;</p> <p>&lt;destination <i>address</i>&gt;</p> <p>&lt;detail&gt;</p> <p>&lt;exp <i>forwarding-class</i>&gt;</p> <p>&lt;logical-system (all   <i>logical-system-name</i>)&gt;</p> <p>reply-mode (application-level-control-channel   ip-udp   no-reply)</p> <p>&lt;size <i>bytes</i>&gt;</p> <p>&lt;source <i>source-address</i>&gt;</p> <p>&lt;sweep&gt;</p>
<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>The <b>size</b> and <b>sweep</b> options were introduced in Junos OS Release 9.6.</p> <p>The <b>reply-mode</b> option and its suboptions are introduced in Junos OS Release 10.4R1.</p>
<b>Description</b>	<p>Check the operability of MPLS Layer 2 virtual private network (VPN) connections. Type Ctrl+c to interrupt a <b>ping mpls l2vpn</b> command.</p>
<b>Options</b>	<p><b>bottom-label-ttl</b>—(Optional) Display the time-to-live value for the bottom label in the label stack.</p> <p><b>count</b> <i>count</i>—(Optional) Number of ping requests to send. If <b>count</b> is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.</p> <p><b>destination</b> <i>address</i>—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.</p> <p><b>detail</b>—(Optional) Display detailed information about the echo requests sent and received.</p> <p><b>exp</b> <i>forwarding-class</i>—(Optional) Value of the forwarding class for the MPLS ping packets.</p> <p><b>instance</b> <i>instance-name</i> local-site-id <i>local-site-id-number</i> remote-site-id <i>remote-site-id-number</i>—Ping 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 ingress and egress provider edge (PE) routers or switches.</p> <p><b>interface</b> <i>interface-name</i>—Ping an interface configured for the Layer 2 VPN on the egress PE router or switch.</p> <p><b>logical-system</b> (all   <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on the specified logical system.</p> <p><b>reply-mode</b>—(Optional) Reply mode for the ping request. This option has the following suboptions:</p> <p><b>application-level-control-channel</b>—Reply using an application level control channel.</p>



**ip-udp**—Reply using an IPv4 or IPv6 UDP packet.

**no-reply**—Do not reply to the ping request.

The **reply-mode** option and its suboptions **application-level-control-channel**, **ip-udp**, and **no-reply** are also available in Junos OS Release 10.2R4 and 10.3R2.

**size bytes**—(Optional) Size of the label-switched path (LSP) ping request packet (96 through 65468 bytes). Packets are 4-byte aligned. For example, If you enter a size of 97, 98, 99, or 100, the router or switch uses a size value of 100 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 96-byte minimum.

**source source-address**—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

<b>Additional Information</b>	<p>You must configure MPLS at the <b>[edit protocols mpls]</b> hierarchy level on the egress PE router or switch (the router or switch receiving the MPLS echo packets) to ping a Layer 2 circuit.</p> <p>In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.</p>
<b>Required Privilege Level</b>	network
<b>List of Sample Output</b>	<p><a href="#">ping mpls l2vpn instance on page 1627</a>  <a href="#">ping mpls l2vpn instance detail on page 1628</a>  <a href="#">ping mpls l2vpn interface &lt;interface-name&gt; reply-mode on page 1628</a></p>
<b>Output Fields</b>	<p>When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code these packets are not counted in the received packets count. They are accounted for separately.</p>

## Sample Output

### ping mpls l2vpn instance

```
user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

### ping mpls l2vpn instance detail

```
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
```

### ping mpls l2vpn interface <interface-name> reply-mode

```
user@host> ping mpls l2vpn interface lt-1/2/0.21 reply-mode ip-udp
!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping mpls l3vpn

**Syntax** ping mpls l3vpn prefix *prefix-name*  
 <*l3vpn-name*>  
 <bottom-label-ttl>  
 <count *count*>  
 <destination *address*>  
 <detail>  
 <exp *forwarding-class*>  
 <logical-system (all | *logical-system-name*)>  
 <size *bytes*>  
 <source *source-address*>  
 <sweep>

**Release Information** Command introduced before Junos OS Release 7.4.  
 Command introduced in Junos OS Release 9.0 for EX Series switches.  
 The **size** and **sweep** options were introduced in Junos OS Release 9.6.  
 Statement introduced in Junos OS Release 12.3X50 for the QFX Series.

**Description** Check the operability of a MPLS Layer 3 virtual private network (VPN) connection. Type Ctrl+c to interrupt a **ping mpls l3vpn** command.

**Options** **bottom-label-ttl**—(Optional) Display the time-to-live value for the bottom label in the label stack.

**count** *count*—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.

**destination** *address*—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.

**detail**—(Optional) Display detailed information about the echo requests sent and received.

**exp** *forwarding-class*—(Optional) Value of the forwarding class for the MPLS ping packets.

**l3vpn-name**—(Optional) Layer 3 VPN name.

**logical-system** (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on the specified logical system.

**prefix** *prefix-name*—Ping to test whether a prefix is present in a provider edge (PE) router's or switch's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix. This option does not test the connection between a PE router or switch and a customer edge (CE) router or switch.

**size** *bytes*—(Optional) Size of the label-switched path (LSP) ping request packet (96 through 65468 bytes). Packets are 4-byte aligned. For example, If you enter a size of 97, 98, 99, or 100, the router or switch uses a size value of 100 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 96-byte minimum.

**source *source-address***—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**Additional Information** You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the egress PE router or switch (the router or switch receiving the MPLS echo packets) to ping a Layer 2 circuit.

In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

If the Layer 3 VPN traffic transits a route reflector within the network, the **ping mpls l3vpn** command does not work.

**Required Privilege Level** network

**List of Sample Output** [ping mpls l3vpn on page 1630](#)  
[ping mpls l3vpn detail on page 1630](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code these packets are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls l3vpn

```
user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32
!!!!
--- 1sping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

### ping mpls l3vpn detail

```
user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32 detail
Request for seq 1, to interface 68, labels <100128, 100112>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <100128, 100112>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <100128, 100112>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <100128, 100112>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <100128, 100112>
Reply for seq 5, return code: Egress-ok
--- 1sping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```



## ping mpls ldp

<b>Syntax</b>	<pre>ping mpls ldp <i>fec</i> &lt;count <i>count</i>&gt; &lt;destination <i>address</i>&gt; &lt;detail&gt; &lt;exp <i>forwarding-class</i>&gt; &lt;instance <i>routing-instance-name</i>&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;p2mp root-addr <i>ip-address</i> lsp-id <i>identifier</i>&gt; &lt;size <i>bytes</i>&gt; &lt;source <i>source-address</i>&gt; &lt;sweep&gt;</pre>
<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>size</b> and <b>sweep</b> options introduced in Junos OS Release 9.6.</p> <p><b>instance</b> option introduced in Junos OS Release 10.0.</p> <p><b>p2mp</b>, <b>root-address</b>, and <b>lsp-id</b> options introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3X50 for the QFX Series.</p>
<b>Description</b>	<p>Check the operability of MPLS LDP-signaled label-switched path (LSP) connections. Type Ctrl+c to interrupt a <b>ping mpls</b> command.</p>
<b>Options</b>	<p><b>count</b> <i>count</i>—(Optional) Number of ping requests to send. If <b>count</b> is not specified, five ping requests are sent. The range of values is 1 through <b>1,000,000</b>. The default value is <b>5</b>.</p> <p><b>destination</b> <i>address</i>—(Optional) Specify an address other than the default (<b>127.0.0.1/32</b>) for the ping echo requests. The address can be anything within the <b>127/8</b> subnet.</p> <p><b>detail</b>—(Optional) Display detailed information about the echo requests sent and received.</p> <p><b>exp</b> <i>forwarding-class</i>—(Optional) Value of the forwarding class for the MPLS ping packets.</p> <p><b>fec</b>—Ping an LDP-signaled LSP using the forwarding equivalence class (FEC) prefix and length.</p> <p><b>instance</b> <i>routing-instance-name</i>—(Optional) Allows you to ping a combination of the routing instance and forwarding equivalence class (FEC) associated with an LSP.</p> <p><b>logical-system</b> (all   <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on the specified logical system.</p> <p><b>p2mp root-addr</b> <i>ip-address</i> <b>lsp-id</b> <i>identifier</i>—(Optional) Ping the end points of a point-to-multipoint LSP. Enter the IP address of the point-to-multipoint LSP root and the ID number of the point-to-multipoint LSP.</p> <p><b>size</b> <i>bytes</i>—(Optional) Size of the LSP ping request packet (<b>88</b> through <b>65468</b> bytes). Packets are 4-byte aligned. For example, If you enter a size of 89, 90, 91, or 92, the router or switch uses a size value of 92 bytes. If you enter a packet size that is smaller</p>

than the minimum size, an error message is displayed reminding you of the 88-byte minimum.

**source *source-address***—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**Additional Information** If the LSP changes, the label and interface information displayed when you issued the **ping** command continues to be used. You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the remote router or switch to ping an LSP terminating there. You must configure MPLS even if you intend to ping only LDP forwarding equivalence classes (FECs).

You can configure the ping interval for the **ping mpls ldp** command by specifying a new time in seconds using the **lsp-ping-interval** statement at the **[edit protocols ldp oam]** hierarchy level. For more information, see the *MPLS Feature Guide for Security Devices*.

In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

**Required Privilege Level** network

**List of Sample Output** [ping mpls ldp fec count on page 1633](#)  
[ping mpls ldp p2mp root-addr lsp-id on page 1633](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with error codes are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls ldp fec count

```
user@host> ping mpls ldp 10.255.245.222 count 10
!!!xxx...x--- lsping statistics ---10 packets transmitted, 3 packets received,
70% packet loss 4 packets received with error status, not counted as received.
```

### ping mpls ldp p2mp root-addr lsp-id

```
user@host> ping mpls ldp p2mp root-addr 10.1.1.1/32 lsp-id 1 count 1
Request for seq 1, to interface 71, no label stack.
Request for seq 1, to interface 70, label 299786
Reply for seq 1, egress 10.1.1.3, return code: Egress-ok, time: 18.936 ms
 Local transmit time: 2009-01-12 03:50:03 PST 407.281 ms
 Remote receive time: 2009-01-12 03:50:03 PST 426.217 ms
Reply for seq 1, egress 10.1.1.4, return code: Egress-ok, time: 18.936 ms
```

```
Local transmit time: 2009-01-12 03:50:03 PST 407.281 ms
Remote receive time: 2009-01-12 03:50:03 PST 426.217 ms
Reply for seq 1, egress 10.1.1.5, return code: Egress-ok, time: 18.936 ms
Local transmit time: 2009-01-12 03:50:03 PST 407.281 ms
Remote receive time: 2009-01-12 03:50:03 PST 426.217 ms
```



## ping mpls lsp-end-point

<b>Syntax</b>	<pre>ping mpls lsp-end-point <i>prefix-name</i> &lt;count <i>count</i>&gt; &lt;destination <i>address</i>&gt; &lt;detail&gt; &lt;exp <i>forwarding-class</i>&gt; &lt;instance <i>routing-instance-name</i>&gt; &lt;logical-system (all   <i>logical-system-name</i>)&gt; &lt;size <i>bytes</i>&gt; &lt;source <i>source-address</i>&gt; &lt;sweep&gt;</pre>
<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>The <b>size</b> and <b>sweep</b> options were introduced in Junos OS Release 9.6.</p> <p>The <b>instance</b> option was introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3X50 for the QFX Series.</p>
<b>Description</b>	<p>Check the operability of MPLS label-switched path (LSP) endpoint connections. Type Ctrl+c to interrupt a <b>ping mpls</b> command.</p>
<b>Options</b>	<p><b>count</b> <i>count</i>—(Optional) Number of ping requests to send. If <b>count</b> is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.</p> <p><b>destination</b> <i>address</i>—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.</p> <p><b>detail</b>—(Optional) Display detailed information about the echo requests sent and received.</p> <p><b>exp</b> <i>forwarding-class</i>—(Optional) Value of the forwarding class for the MPLS ping packets.</p> <p><b>instance</b> <i>routing-instance-name</i>—(Optional) Ping a combination of the routing instance and forwarding equivalence class (FEC) associated with an LSP connection.</p> <p><b>logical-system</b> (all   <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on the specified logical system.</p> <p><b>prefix-name</b>—LDP forwarding equivalence class (FEC) prefix or RSVP LSP endpoint address.</p> <p><b>size</b> <i>bytes</i>—(Optional) Size of the LSP ping request packet. If the endpoint is LDP-based, the minimum size of the packet is 88 bytes. If the endpoint is RSVP-based, the minimum size of the packet is 100 bytes. The maximum size in either case is 65468 bytes.</p> <p><b>source</b> <i>source-address</i>—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (lo.0).</p>

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**Additional Information** If the LSP changes, the label and interface information displayed when you issued the **ping** command continues to be used. You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the remote router or switch to ping an LSP terminating there. You must configure MPLS even if you intend to ping only LDP forwarding equivalence classes (FECs).

In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

**Required Privilege Level** network

**List of Sample Output** [ping mpls lsp-end-point detail on page 1636](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with an error code are not counted in the received packets count. They are accounted for separately.

## Sample Output

### [ping mpls lsp-end-point detail](#)

```
user@host> ping mpls lsp-end-point 10.255.245.119 detail
Route to end point address is via LDP FEC
Request for seq 1, to interface 67, label 100032
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 67, label 100032
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 67, label 100032
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 67, label 100032
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 67, label 100032
Reply for seq 5, return code: Egress-ok
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping mpls rsvp

**Syntax** ping mpls rsvp  
 <lsp-name>  
 <count count>  
 <destination address>  
 <detail>  
 <dynamic-bypass>  
 <egress egress-address>  
 <exp forwarding-class>  
 <interface interface-name>  
 <logical-system (all | logical-system-name)>  
 <manual-bypass>  
 <multipoint>  
 <size bytes>  
 <source source-address>  
 <standby standby-path-name>  
 <sweep>

**Release Information** Command introduced before Junos OS Release 7.4.  
 The **egress** and **multipoint** options were introduced in Junos OS Release 9.2.  
 The **size** and **sweep** options were introduced in Junos OS Release 9.6.  
 The **dynamic-bypass** and **manual-bypass** options were introduced in Junos OS Release 10.2.  
 Statement introduced in Junos OS Release 12.3X50 for the QFX Series.

**Description** Check the operability of MPLS RSVP-signaled label-switched path (LSP) connections. Type Ctrl+c to interrupt a **ping mpls** command.

**Options** **count count**—(Optional) Number of ping requests to send. If **count** is not specified, five ping requests are sent. The range of values is 1 through 1,000,000. The default value is 5.

**destination address**—(Optional) Specify an address other than the default (127.0.0.1/32) for the ping echo requests. The address can be anything within the 127/8 subnet.

**detail**—(Optional) Display detailed information about the echo requests sent and received.



**NOTE:** When using the **detail** option, the reported time is based on the system time configured on the local and remote routers. Differences in these system times can result in inaccurate one way ping trip times being reported.

In practice, it is difficult to synchronize the system times of independent Juniper Networks routers with sufficient accuracy to provide a meaningful time value for the **detail** option (even when synchronized using NTP).

**dynamic-bypass**—(Optional) Ping dynamically generated bypass LSPs, used for protecting other LSPs.

**egress *egress-address***—(Optional) Only the specified egress router or switch responds to the ping request.

**exp *forwarding-class***—(Optional) Value of the forwarding class for the MPLS ping packets.

**interface**—(Optional) Specify the name of the interface protected by the manual bypass LSP. This option is only available when you have also used the **manual-bypass** option.

**logical-system (all | *logical-system-name*)**—(Optional) Perform this operation on all logical systems or on the specified logical system.

***lsp-name***—Ping an RSVP-signaled LSP using an LSP name.

**manual-bypass**—(Optional) Ping manually configured bypass LSPs, used for protecting other LSPs. For this option, you must also specify the interface protected by the manual bypass LSP using the **interface** option.

**multipoint**—(Optional) Send ping requests to each of the egress routers or switches participating in a point-to-multipoint LSP. You can also include the **egress** option to ping a specific egress router or switch participating in a point-to-multipoint LSP.

**size *bytes***—(Optional) Size of the LSP ping request packet (100 through 65468 bytes). Packets are 4-byte aligned. For example, if you enter a size of 101, 102, 103, or 104, the router or switch uses a size value of 104 bytes. If you enter a packet size that is smaller than the minimum size, an error message is displayed reminding you of the 100-byte minimum.

**source *source-address***—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface.

**standby *standby-path-name***—(Optional) Name of the standby path.

**sweep**—(Optional) Automatically determine the size of the maximum transmission unit (MTU).

**Additional Information** If the LSP changes, the label and interface information displayed when you issued the **ping** command continues to be used. You must configure MPLS at the **[edit protocols mpls]** hierarchy level on the remote router or switch to ping an LSP terminating there. You must configure MPLS even if you intend to ping only LDP forwarding equivalence classes (FECs).

In asymmetric MTU scenarios, the echo response may be dropped. For example, if the MTU from System A to System B is 1000 bytes, the MTU from System B to System A is 500 bytes, and the ping request packet size is 1000 bytes, the echo response is dropped because the PAD TLV is included in the echo response, making it too large.

**Required Privilege Level** network

**List of Sample Output** [ping mpls rsvp \(Echo Reply Received\) on page 1639](#)  
[ping mpls rsvp \(Echo Reply with Error Code\) on page 1639](#)

[ping mpls rsvp detail on page 1639](#)

[ping mpls rsvp multipoint egress detail count on page 1639](#)

[ping mpls rsvp multipoint detail count on page 1639](#)

[ping mpls rsvp destination detail count size on page 1640](#)

[ping mpls rsvp destination detail sweep size on page 1640](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. Packets with an error code are not counted in the received packets count. They are accounted for separately.

## Sample Output

### ping mpls rsvp (Echo Reply Received)

```
user@host> ping mpls rsvp test1
!!!!!--- lsping statistics ---5 packets transmitted, 5 packets received, 0% packet
loss
```

### ping mpls rsvp (Echo Reply with Error Code)

```
user@host> ping mpls rsvp test2
!!xxx--- lsping statistics ---5 packets transmitted, 2 packets received, 60%
packet loss3 packets received with error status, not counted as received.
```

### ping mpls rsvp detail

```
user@host> ping mpls rsvp to-green detail
Request for seq 1, to interface 67, labels <100095, 0, 0>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 67, labels <100095, 0, 0>
Reply for seq 2, return code: Egress-ok
```

### ping mpls rsvp multipoint egress detail count

```
user@host>ping mpls rsvp sample-lsp multipoint egress 192.168.1.3 detail count 1
Request for seq 1, to interface 70, label 299952
Request for seq 1, to interface 70, no label stack.
Request for seq 1, to interface 67, no label stack.

Reply for seq 1, egress 192.168.1.3, return code: Egress-ok, time: 0.242 ms
Local transmit time: 1205310695s 215737us
Remote receive time: 1205310695s 215979us

--- lsping, egress 192.168.1.3 statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
```

### ping mpls rsvp multipoint detail count

```
user@host>ping mpls rsvp sample-lsp multipoint detail count 1
Request for seq 1, to interface 70, label 299952
Request for seq 1, to interface 70, no label stack.
Request for seq 1, to interface 67, no label stack.

Reply for seq 1, return code: Unknown TLV, time: 9.877 ms
Local transmit time: 1205310615s 347317us
Remote receive time: 1205310615s 357194us
Reply for seq 1, egress 192.168.1.3, return code: Egress-ok, time: 0.351 ms
```

```

Local transmit time: 1205310615s 347262us
Remote receive time: 1205310615s 347613us
Reply for seq 1, egress 192.168.1.13, return code: Egress-ok, time: 0.301 ms
Local transmit time: 1205310615s 347167us
Remote receive time: 1205310615s 347468us
Timeout for seq 1, egress 192.168.1.1
Timeout for seq 1, egress 192.168.1.4
Timeout for seq 1, egress 192.168.1.14

--- lsping, egress 192.168.1.1 statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

--- lsping, egress 192.168.1.3 statistics ---
1 packets transmitted, 1 packets received, 0% packet loss

--- lsping, egress 192.168.1.4 statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

--- lsping, egress 192.168.1.13 statistics ---
1 packets transmitted, 1 packets received, 0% packet loss

--- lsping, egress 192.168.1.14 statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

```

#### ping mpls rsvp destination detail count size

```

user@host> ping mpls rsvp chaser-access destination 192.168.0.1 detail count 1 size 4468

Request for seq 1, to interface 88, label 299984, packet size 4468
Reply for seq 1, return code: Egress-ok, time: 44.804 ms
 Local transmit time: 2009-03-30 22:05:02 CEST 408.629 ms
 Remote receive time: 2009-03-30 22:05:02 CEST 453.433 ms

--- lsping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss

```

#### ping mpls rsvp destination detail sweep size

```

user@router> ping mpls rsvp chaser-access destination 192.168.0.1 detail sweep size 4500
Request for seq 1, to interface 86, no label stack., packet size 100
Reply for seq 1, return code: Egress-ok, time: -39.264 ms
 Local transmit time: 2009-04-24 14:05:40 CEST 541.423 ms
 Remote receive time: 2009-04-24 14:05:40 CEST 502.159 ms
Request for seq 2, to interface 86, no label stack., packet size 2300
Reply for seq 2, return code: Egress-ok, time: -38.179 ms
 Local transmit time: 2009-04-24 14:05:41 CEST 544.240 ms
 Remote receive time: 2009-04-24 14:05:41 CEST 506.061 ms
Request for seq 3, to interface 86, no label stack., packet size 4500
Timeout for seq 3
Request for seq 4, to interface 86, no label stack., packet size 3400
Reply for seq 4, return code: Egress-ok, time: -37.545 ms
 Local transmit time: 2009-04-24 14:05:45 CEST 549.953 ms
 Remote receive time: 2009-04-24 14:05:45 CEST 512.408 ms
Request for seq 5, to interface 86, no label stack., packet size 3952
Reply for seq 5, return code: Egress-ok, time: -37.176 ms
 Local transmit time: 2009-04-24 14:05:46 CEST 555.881 ms
 Remote receive time: 2009-04-24 14:05:46 CEST 518.705 ms
Request for seq 6, to interface 86, no label stack., packet size 4228
Reply for seq 6, return code: Egress-ok, time: -36.962 ms
 Local transmit time: 2009-04-24 14:05:47 CEST 561.809 ms
 Remote receive time: 2009-04-24 14:05:47 CEST 524.847 ms

```

```
Request for seq 7, to interface 86, no label stack., packet size 4368
Reply for seq 7, return code: Egress-ok, time: -36.922 ms
 Local transmit time: 2009-04-24 14:05:48 CEST 568.738 ms
 Remote receive time: 2009-04-24 14:05:48 CEST 531.816 ms
Request for seq 8, to interface 86, no label stack., packet size 4440
Reply for seq 8, return code: Egress-ok, time: -36.855 ms
 Local transmit time: 2009-04-24 14:05:49 CEST 575.669 ms
 Remote receive time: 2009-04-24 14:05:49 CEST 538.814 ms
Request for seq 9, to interface 86, no label stack., packet size 4476
Timeout for seq 9
Request for seq 10, to interface 86, no label stack., packet size 4460
Reply for seq 10, return code: Egress-ok, time: -36.906 ms
 Local transmit time: 2009-04-24 14:05:53 CEST 584.382 ms
 Remote receive time: 2009-04-24 14:05:53 CEST 547.476 ms
Request for seq 11, to interface 86, no label stack., packet size 4480
Timeout for seq 11
Request for seq 12, to interface 86, no label stack., packet size 4472
Timeout for seq 12
Request for seq 13, to interface 86, no label stack., packet size 4468
Reply for seq 13, return code: Egress-ok, time: -36.943 ms
 Local transmit time: 2009-04-24 14:06:00 CEST 594.884 ms
 Remote receive time: 2009-04-24 14:06:00 CEST 557.941 ms
Request for seq 14, to interface 86, no label stack., packet size 4476
Timeout for seq 14
Request for seq 15, to interface 86, no label stack., packet size 4472
Timeout for seq 15

--- lsp ping sweep result---
Maximum Transmission Unit (MTU) is 4468 bytes
```

## request pppoe connect

---

<b>Syntax</b>	request pppoe connect
<b>Release Information</b>	Statement supported on SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 is introduced in Release 11.2 and 11.4 of Junos OS.
<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 1642</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 SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 is introduced in Release 11.2 and 11.4 of Junos OS.
<b>Description</b>	Connect all sessions that are down.
<b>Options</b>	<b>session id</b> — (Optional) Disconnect the session for which the session ID is specified. <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 1643</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

---

Syntax	request services ip-monitoring preempt-restore policy <policy-name>
Release Information	Command introduced in Release 11.4 of Junos OS.
Description	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> <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.</div>
Options	policy name—Name of the policy.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">show services rpm probe-results (View) on page 1707</a></li><li>• <a href="#">show services ip-monitoring status on page 1703</a></li></ul>
List of Sample Output	<a href="#">run request services ip-monitoring preempt-restore policy &lt;policy name&gt; on page 1644</a>
Output Fields	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
```

## 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 1711</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show chassis alarms on page 1645</a>
<b>Output Fields</b>	<a href="#">Table 231 on page 1645</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 231: 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 configuration

---

<b>Syntax</b>	show configuration <statement-path>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display the configuration that currently is running on the router or switch, which is the last committed configuration.
<b>Options</b>	<p><b>none</b>—Display the entire configuration.</p> <p><b>statement-path</b>—(Optional) Display one of the following hierarchies in a configuration. (Each <b>statement-path</b> 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"> <li>• <b>access</b>—Network access configuration.</li> <li>• <b>access-profile</b>—Access profile configuration.</li> <li>• <b>accounting-options</b>—Accounting data configuration.</li> <li>• <b>applications</b>—Applications defined by protocol characteristics.</li> <li>• <b>apply-groups</b>—Groups from which configuration data is inherited.</li> <li>• <b>chassis</b>—Chassis configuration.</li> <li>• <b>chassis network-services</b>—Current running mode.</li> <li>• <b>class-of-service</b>—Class-of-service configuration.</li> <li>• <b>diameter</b>—Diameter base protocol layer configuration.</li> <li>• <b>ethernet-switching-options</b>—(EX Series switch only) Ethernet switching configuration.</li> <li>• <b>event-options</b>—Event processing configuration.</li> <li>• <b>firewall</b>—Firewall configuration.</li> <li>• <b>forwarding-options</b>—Options that control packet sampling.</li> <li>• <b>groups</b>—Configuration groups.</li> <li>• <b>interfaces</b>—Interface configuration.</li> <li>• <b>jsrc</b>—JSRC partition configuration.</li> <li>• <b>jsrc-partition</b>—JSRC partition configuration.</li> <li>• <b>logical-systems</b>—Logical system configuration.</li> <li>• <b>poe</b>—(EX Series switch only) Power over Ethernet configuration.</li> <li>• <b>policy-options</b>—Routing policy option configuration.</li> <li>• <b>protocols</b>—Routing protocol configuration.</li> </ul>

- **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 363](#)
- [Overview of Junos OS CLI Operational Mode Commands on page 413](#)

**List of Sample Output** [show configuration on page 1648](#)  
[show configuration policy-options on page 1649](#)

**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 alant version "8.2IO [builder]";
last changed: 2006-10-31 14:05:53 PST
system {
 host-name exhost;
 domain-name example.net;
 backup-router 192.1.1.254;
 time-zone America/Los_Angeles;
 default-address-selection;
 name-server {
 192.154.169.254;
 192.154.169.249;
```

```

 192.154.169.176;
 }
 services {
 telnet;
 }
 tacplus-server {
 1.2.3.4 {
 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 chassis cluster ip-monitoring status redundancy-group

<b>Syntax</b>	<b>show chassis cluster ip-monitoring status</b> <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><i>redundancy-group (Interfaces)</i></li> <li><i>clear chassis cluster failover-count</i></li> <li><i>request chassis cluster failover node</i></li> <li><i>request chassis cluster failover reset</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show chassis cluster ip-monitoring status on page 1651</a> <a href="#">show chassis cluster ip-monitoring status redundancy-group on page 1652</a>
<b>Output Fields</b>	<a href="#">Table 232 on page 1650</a> lists the output fields for the <b>show chassis cluster ip-monitoring status</b> command.

**Table 232: 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.



Table 232: show chassis cluster ip-monitoring status Output Fields (*continued*)

Field Name	Field Description
Reason	Explanation for the reported status. See <a href="#">Table 233 on page 1651</a> .
Weight	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 233: 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 may 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.  or  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*)  
 }

**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.

**Required Privilege Level**    view

**Related Documentation**    • *Understanding Interfaces*

List of Sample Output	<a href="#">show interfaces Gigabit Ethernet</a> on page 1662
	<a href="#">show interfaces brief (Gigabit Ethernet)</a> on page 1663
	<a href="#">show interfaces detail (Gigabit Ethernet)</a> on page 1663
	<a href="#">show interfaces extensive (Gigabit Ethernet)</a> on page 1665
	<a href="#">show interfaces terse</a> on page 1668
	<a href="#">show interfaces controller (Channelized E1 IQ with Logical E1)</a> on page 1668
	<a href="#">show interfaces controller (Channelized E1 IQ with Logical DSO)</a> on page 1668
	<a href="#">show interfaces descriptions</a> on page 1669
	<a href="#">show interfaces destination-class all</a> on page 1669
	<a href="#">show interfaces diagnostics optics</a> on page 1669
	<a href="#">show interfaces far-end-interval coc12-5/2/0</a> on page 1670
	<a href="#">show interfaces far-end-interval coc1-5/2/1:1</a> on page 1670
	<a href="#">show interfaces filters</a> on page 1671
	<a href="#">show interfaces flow-statistics (Gigabit Ethernet)</a> on page 1671
	<a href="#">show interfaces interval (Channelized OC12)</a> on page 1672
	<a href="#">show interfaces interval (E3)</a> on page 1672
	<a href="#">show interfaces interval (SONET/SDH)</a> on page 1673
	<a href="#">show interfaces load-balancing</a> on page 1673
	<a href="#">show interfaces load-balancing detail</a> on page 1673
	<a href="#">show interfaces mac-database (All MAC Addresses on a Port)</a> on page 1674
	<a href="#">show interfaces mac-database (All MAC Addresses on a Service)</a> on page 1674
	<a href="#">show interfaces mac-database mac-address</a> on page 1675
	<a href="#">show interfaces mc-ae</a> on page 1675
	<a href="#">show interfaces media (SONET/SDH)</a> on page 1675
	<a href="#">show interfaces policers</a> on page 1676
	<a href="#">show interfaces policers interface-name</a> on page 1676
	<a href="#">show interfaces queue</a> on page 1676
	<a href="#">show interfaces redundancy</a> on page 1677
	<a href="#">show interfaces redundancy (Aggregated Ethernet)</a> on page 1677
	<a href="#">show interfaces redundancy detail</a> on page 1678
	<a href="#">show interfaces routing brief</a> on page 1678
	<a href="#">show interfaces routing detail</a> on page 1678
	<a href="#">show interfaces routing-instance all</a> on page 1679
	<a href="#">show interfaces snmp-index</a> on page 1679
	<a href="#">show interfaces source-class all</a> on page 1679
	<a href="#">show interfaces statistics (Fast Ethernet)</a> on page 1680
	<a href="#">show interfaces switch-port</a> on page 1680
	<a href="#">show interfaces transport pm</a> on page 1681

**Output Fields** [Table 234 on page 1655](#) lists the output fields for the **show interfaces** command. Output fields are listed in the approximate order in which they appear.

**Table 234: show interfaces Output Fields**

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface.	All levels

Table 234: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<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>
<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

Table 234: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Active alarms and Active defects	<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>	detail extensive none
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<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>	detail extensive
Input errors	<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>	extensive

Table 234: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<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>
<b>Ingress queues</b>	Total number of ingress queues supported on the specified interface.	<b>extensive</b>
<b>Queue counters and queue number</b>	<p>CoS queue number and its associated user-configured forwarding class name.</p> <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>



Table 234: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
MAC statistics	<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</b> and <b>total packets</b>—Total number of octets and packets.</li> <li>• <b>Unicast packets</b>, <b>Broadcast packets</b>, and <b>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>	extensive

Table 234: 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 234: 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 234: 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.  <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: 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 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:

```





```

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: Sendbcast-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 10.0.0.16	--> 0/0 --> 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 any
ge-5/0/0.0 up up inet
 multiservice
 f-any
 f-inet
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
Is ping
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
ge-0/0/0.0 up up inet
 up up 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
 up up 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
 up down iso
 up down 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 : 6250000 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	NA
Lane differential group delay	0	0	0	0	0
0	NA	NA	NA	NA	NA
q Value	120	120	120	120	0
0	NA	NA	NA	NA	NA
SNR	28	28	29	28	0
0	NA	NA	NA	NA	NA
Tx output power(0.01dBm)	-5000	-5000	-5000	-5000	-300
-100	No	No	No	No	No
Rx input power(0.01dBm)	-3642	-3665	-3626	-3637	-1800
-500	No	No	No	No	No
Module temperature(Celsius)	46	46	46	46	-5
75	No	No	No	No	No
Tx laser bias current(0.1mA)	0	0	0	0	0
0	NA	NA	NA	NA	NA
Rx laser bias current(0.1mA)	1270	1270	1270	1270	0
0	NA	NA	NA	NA	NA
Carrier frequency offset(MHz)	-186	-186	-186	-186	-5000
5000	No	No	No	No	No



## show poe interface (View)

<b>Syntax</b>	show poe interface <ge-fpc/pic/port>
<b>Release Information</b>	Command introduced in Release 9.5 of Junos OS.
<b>Description</b>	Display the status of Power over Ethernet (PoE) ports.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>none</b>—Display the status of all PoE ports on the SRX Series device.</li> <li>• <b>ge-fpc/pic/port</b>— (Optional) Display the status of a specific PoE port on the SRX Series device.</li> </ul>
<b>Required Privilege Level</b>	View
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring PoE on All Interfaces</i></li> </ul>
<b>Output Fields</b>	Table 235 on page 1683 lists the output fields for the <b>show poe interface</b> command. Output fields are listed in the approximate order in which they appear.

**Table 235: show poe interface Output Fields**

Field name	Field Description
PoE Interface	Specifies the interface name.
Admin Status	Specifies whether PoE capabilities are enabled or disabled.
Oper status	Specifies the operational status of the port.
Max-power	Specifies the maximum power configured on the port.
Priority	Specifies whether the port is high priority or low priority.
Power-consumption	Specifies how much power is being used by the port.
Class	Indicates the class of the powered device as defined by the IEEE 802 AF standard.

## Sample Output

### show poe interface

```
user@host>show poe interface
```

```

Interface Admin status Oper status Max power Priority Power consumption Class
ge-0/0/0 Enabled Searching 15.4W Low 0.0W 0
ge-0/0/1 Enabled Powered-up 15.4W High 6.6W 0
ge-0/0/2 Disabled Disabled 15.4W Low 0.0W 0
ge-0/0/3 Disabled Disabled 15.4W Low 0.0W 0

```

```
user@host>show poe interface ge-0/0/1
```

```
PoE interface status :
PoE interface : ge-0/0/1
Administrative status : Enabled
Operational status : Powered-up
Power limit on the interface : 15.4 W
Priority : High
Power consumed : 6.6 W
Class of power device : 0
```

## show poe telemetries

<b>Syntax</b>	show poe telemetries <interface <i>interface-name</i> count <i>number</i> > <count <i>number</i> interface <i>interface-name</i> >
<b>Release Information</b>	Command modified in Junos OS Release 12.3X48-D10.
<b>Description</b>	Display a history of power consumption on the specified interface. Telemetries must be enabled on the interface before you can display a history of power consumption.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>Interface <i>interface-name</i></b>—Display telemetries for the specified PoE interface.</li> <li>• <b>count <i>number</i></b>—Display the specified number of telemetries records for the specified PoE interface.</li> </ul>
<b>Required Privilege Level</b>	View
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Configuring PoE on All Interfaces</i></li> </ul>
<b>Output Fields</b>	Table 236 on page 1685 lists the output fields for the <b>show poe telemetries interface</b> command. Output fields are listed in the approximate order in which they appear.

Table 236: show poe telemetries interface Output Fields

Field name	Field Description
S1 No	Number of the record for the specified port. The last record is the most recent.
Timestamp	Time that the power-consumption data was gathered.
Power	Amount of power provided by the specified port at the time the data was gathered.
Voltage	Voltage on the specified port at the time the data was gathered.

## Sample Output

### show poe telemetries interface

```
user@host>show poe telemetries interface ge-0/0/1 count 8
```

S1 No	Timestamp	Power	Voltage
1	Fri Jan 04 11:41:15 2009	6.6 W	47.2 V
2	Fri Jan 04 11:40:15 2009	6.6 W	47.2 V
3	Fri Jan 04 11:39:15 2009	6.6 W	47.2 V
4	Fri Jan 04 11:38:15 2009	6.6 W	47.2 V
5	Fri Jan 04 11:37:15 2009	6.6 W	47.2 V
6	Fri Jan 04 11:36:15 2009	6.6 W	47.2 V
7	Fri Jan 04 11:35:15 2009	6.6 W	47.2 V

8 Fri Jan 04 11:34:15 2009 6.6 W 47.2 V

**user@host>show poe telemetries count 5 interface ge-0/0/1**

S1 No	Timestamp	Power	Voltage
1	Fri Jan 04 11:47:15 2009	6.6 W	47.2 V
2	Fri Jan 04 11:38:15 2009	6.6 W	47.2 V
3	Fri Jan 04 11:29:15 2009	6.6 W	47.2 V
4	Fri Jan 04 11:11:15 2009	6.6 W	47.2 V
5	Fri Jan 04 11:10:15 2009	6.6 W	47.2 V

## show pppoe interfaces

<b>Syntax</b>	show pppoe interfaces <brief   detail   extensive> <pp0.logical>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5.
<b>Description</b>	Display session-specific information about PPPoE interfaces.
<b>Options</b>	<p><b>none</b>—Display interface information for all PPPoE interfaces.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>extensive</b>—(Optional) Display information about the number of packets sent and received and the number of timeouts during a PPPoE session.</p> <p><b>pp0.logical</b>—(Optional) Name of an interface. The logical unit number for static interfaces can be a value from 0 through 16385. The logical unit number for dynamic interfaces can be a value from 1073741824 through the maximum number of logical interfaces supported on your SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Understanding Ethernet Interfaces</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show pppoe interfaces on page 1688</a> <a href="#">show pppoe interfaces brief on page 1689</a> <a href="#">show pppoe interfaces detail on page 1689</a> <a href="#">show pppoe interfaces extensive on page 1689</a>
<b>Output Fields</b>	Table 237 on page 1687 lists the output fields for the <b>show pppoe interfaces</b> command. Output fields are listed in the approximate order in which they appear.

Table 237: show pppoe interfaces Output Fields

Field Name	Field Description
Index	Index number of the logical interface, which reflects its initialization sequence.
State	State of the logical interface: <b>up</b> or <b>down</b> .
Session ID	Session ID.
Service name	Type of service required (can be used to indicate an ISP name, a class, or quality of service).
Configured AC name	Configured access concentrator name.
Session AC name	Name of the access concentrator.

Table 237: show pppoe interfaces Output Fields (*continued*)

Field Name	Field Description
<b>Remote MAC address or Remote MAC</b>	MAC address of the remote side of the connection, either the access concentrator or the PPPoE client.
<b>Auto-reconnect timeout</b>	Timeout value for reconnecting after a PPPoE session is terminated (in seconds).
<b>Idle timeout</b>	Length of time (in seconds) that a connection can be idle before disconnecting.
<b>Session uptime</b>	Length of time the session has been up, in <i>hh:mm:ss</i> .
<b>Underlying interface</b>	Interface on which PPPoE is running.
<b>Packet Type</b>	<p>Number of packets sent and received during the PPPoE session, categorized by packet type and packet errors:</p> <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 Termination 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 performing 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 packets</b>—Malformed or short packets that caused the packet handler to discard the frame as unreadable.</li> <li>• <b>Unknown packets</b>—Unrecognized packets.</li> </ul>
<b>Timeout</b>	<p>Timeouts that occur during the PPPoE session:</p> <ul style="list-style-type: none"> <li>• <b>PADI</b>—No PADI packets received within the timeout period.</li> <li>• <b>PADO</b>—No PADO packets received within the timeout period. (This value is always zero and is not supported.)</li> <li>• <b>PADR</b>—No PADR packets received within the timeout period.</li> </ul>
<b>Receive Error Counters</b>	<p>Error counters received during the PPPoE session:</p> <ul style="list-style-type: none"> <li>• <b>PADI</b>—No PADI error counters received during the session.</li> <li>• <b>PADO</b>—No PADO error counters received during the session.</li> <li>• <b>PADR</b>—No PADR error counters received during the session.</li> <li>• <b>PADS</b>—No PADS error counters received during the session.</li> </ul>

## Sample Output

### show pppoe interfaces

```
user@host> show pppoe interfaces
```

```

pp0.0 Index 71
State: Session up, Session ID: 4,
Service name: None,
Session AC name: srx-pppoe-ac, Configured AC name: None,
Remote MAC address: b0:c6:9a:74:5e:c1,
Session uptime: 5d 15:21 ago,
Auto-reconnect timeout: Never, Idle timeout: Never,
Underlying interface: ge-0/0/1.0 Index 70

```

#### show pppoe interfaces brief

```

user@host> show pppoe interfaces brief

```

Interface	Underlying interface	State	Session ID	Remote MAC
pp0.0	ge-0/0/1.0	Session up	4	b0:c6:9a:74:5e:c1

#### show pppoe interfaces detail

```

user@host> show pppoe interfaces detail
pp0.0 Index 71
State: Session up, Session ID: 4,
Service name: None,
Session AC name: srx-pppoe-ac, Configured AC name: None,
Remote MAC address: b0:c6:9a:74:5e:c1,
Session uptime: 5d 15:21 ago,
Auto-reconnect timeout: Never, Idle timeout: Never,
Underlying interface: ge-0/0/1.0 Index 70

```

#### show pppoe interfaces extensive

```

user@host> show pppoe interfaces extensive
pp0.0 Index 71
State: Session up, Session ID: 4,
Service name: None,
Session AC name: srx-pppoe-ac, Configured AC name: None,
Remote MAC address: b0:c6:9a:74:5e:c1,
Session uptime: 5d 15:22 ago,
Auto-reconnect timeout: Never, Idle timeout: Never,
Underlying interface: ge-0/0/1.0 Index 70

```

PacketType	Sent	Received
PADI	1	0
PADO	0	1
PADR	1	0
PADS	0	1
PADT	0	0
Service name error	0	0
AC system error	0	0
Generic error	0	0
Malformed packets	0	0
Unknown packets	0	0

```

Timeout
PADI 0
PADO 0
PADR 0
Receive Error Counters
PADI 0
PADO 0
PADR 0
PADS 0

```

## show pppoe statistics

<b>Syntax</b>	<code>show pppoe statistics</code> <code>&lt;logical-interface-name&gt;</code>
<b>Release Information</b>	Command is introduced in Junos OS Release 9.5.
<b>Description</b>	Display statistics information about PPPoE interfaces.
<b>Options</b>	<p><b>none</b>—Display PPPoE statistics for all interfaces.</p> <p><b>logical-interface-name</b>—(Optional) Name of an underlying PPPoE logical interface.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show pppoe interfaces on page 1687</a></li> <li>• <i>Understanding Ethernet Interfaces</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show pppoe statistics on page 1691</a>
<b>Output Fields</b>	Table 238 on page 1690 lists the output fields for the <b>show pppoe statistics</b> command. Output fields are listed in the approximate order in which they appear.

**Table 238: show pppoe statistics Output Fields**

Field Name	Field Description
Active PPPoE sessions	Total number of active PPPoE sessions.
Packet Type	<p>Number of packets sent and received during the PPPoE session, categorized by packet type and packet errors:</p> <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 Termination 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 performing 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 packets</b>—Malformed or short packets that caused the packet handler to discard the frame as unreadable.</li> <li>• <b>Unknown packets</b>—Unrecognized packets.</li> </ul>



Table 238: show pppoe statistics Output Fields (*continued*)

Field Name	Field Description
<b>Timeout</b>	Timeouts that occur during the PPPoE session: <ul style="list-style-type: none"> <li>• <b>PADI</b>—No PADI packets received within the timeout period.</li> <li>• <b>PADO</b>—No PADO packets received within the timeout period. (This value is always zero and is not supported.)</li> <li>• <b>PADR</b>—No PADR packets received within the timeout period.</li> </ul>
<b>Receive Error Counters</b>	Error counters received during the PPPoE session: <ul style="list-style-type: none"> <li>• <b>PADI</b>—No PADI error counters received during the session.</li> <li>• <b>PADO</b>—No PADO error counters received during the session.</li> <li>• <b>PADR</b>—No PADR error counters received during the session.</li> <li>• <b>PADS</b>—No PADS error counters received during the session.</li> </ul>

## Sample Output

### show pppoe statistics

```

user@host> show pppoe statistics
Active PPPoE sessions: 0

PacketType Sent Received
PADI 0 0
PADO 0 0
PADR 0 0
PADS 0 0
PADT 0 0
Service name error 0 0
AC system error 0 0
Generic error 0 0
Malformed packets 0 0
Unknown packets 0 0
Timeout
PADI 0
PADO 0
PADR 0
Receive Error Counters
PADI 0
PADO 0
PADR 0
PADS 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 1694](#)  
[show security alarms detail on page 1694](#)  
[show security alarms alarm-id on page 1694](#)  
[show security alarms alarm-type authentication on page 1694](#)  
[show security alarms newer-than <time> on page 1695](#)  
[show security alarms older-than <time> on page 1695](#)  
[show security alarms process <process> on page 1695](#)  
[show security alarms severity <severity> on page 1695](#)

**Output Fields** [Table 239 on page 1693](#) 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 239: 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 239: 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 '10.17.0.1'
2 2010-01-19 13:41:52 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
3 2010-01-19 13:42:13 PST SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

### 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 '10.17.0.1'
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 '10.17.0.1'
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 '10.17.0.1'
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 '10.17.0.1'
```

### 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 '10.17.0.1'
2	2010-01-19 13:41:52 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'
3	2010-01-19 13:42:13 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'

#### 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 '10.17.0.1'
---	-------------------------	----------------------------------------------------------------------------------------------------------

#### 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 '10.17.0.1'
2	2010-01-19 13:41:52 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'

#### 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 '10.17.0.1'
2	2010-01-19 13:41:52 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'
3	2010-01-19 13:42:13 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'

#### 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 '10.17.0.1'
2	2010-01-19 13:41:52 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'
3	2010-01-19 13:42:13 PST	SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for user 'user' reached from '10.17.0.1'

## show security datapath-debug capture

---

<b>Syntax</b>	show security datapath-debug capture
<b>Release Information</b>	Command introduced in Release 10.0 of Junos OS.
<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 1697</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 capture on page 1696</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 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 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 Release 10.0 of Junos OS.
<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 1696</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 1697</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 fpc fpc-number

<b>Syntax</b>	<b>show security monitoring fpc <i>fpc-number</i></b> <b>&lt;node ( <i>node-id</i>   all   local   primary )&gt;</b>
<b>Release Information</b>	Command introduced in Release 9.2 of Junos OS.
<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 Security 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 1703</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security monitoring fpc 0 on page 1699</a> <a href="#">show security monitoring fpc 1 on page 1699</a> <a href="#">show security monitoring fpc 8 on page 1700</a>
<b>Output Fields</b>	<a href="#">Table 240 on page 1698</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 240: 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 may be a software problem (memory leak).



Table 240: 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 SRX3400, SRX3600, SRX5600, and SRX5800 devices only).
<b>SPU max cp session</b>	The maximum number of cp sessions allowed for the SPU (on SRX3400, SRX3600, 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 Release of 10.2 of Junos OS.

**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 SRX100, SRX210, SRX240, and SRX650 devices.

**Required Privilege Level** View

**Related Documentation**

- [show services ip-monitoring status on page 1703](#)

## 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 Release 10.2 of Junos OS.

**Description** Display the services processing unit (SPU) statistics for all FPC slots over 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 SRX100, SRX210, SRX240, and SRX650 devices.

**Required Privilege Level** View

**Related Documentation**

- [show services ip-monitoring status on page 1703](#)

## show security monitoring performance spu

```
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 Release 11.4 R2 of Junos OS. Next-hop functionality added in Junos OS Release 23.1X46-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) on page 1707</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services ip-monitoring status on page 1704</a> <a href="#">show services ip-monitoring status on page 1704</a> <a href="#">show services ip-monitoring status on page 1705</a> <a href="#">show services ip-monitoring status on page 1705</a> <a href="#">show services ip-monitoring status on page 1705</a>
<b>Output Fields</b>	Table 241 on page 1703 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 241: 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 241: 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 services rpm probe-results (View)

<b>Syntax</b>	show services rpm probe-results <owner <i>owner</i> > <test <i>name</i> >
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Display the results of the most recent real-time performance monitoring (RPM) probes.
<b>Options</b>	<p><b>none</b>—Display all results of the most recent RPM probes.</p> <p><b>owner <i>owner</i></b>—(Optional) Display information for the specified probe owner.</p> <p><b>test <i>name</i></b>—(Optional) Display information for the specified test.</p>
<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 1703</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services rpm probe-results on page 1710</a>
<b>Output Fields</b>	<a href="#">Table 242 on page 1707</a> lists the output fields for the <b>show services rpm probe-results</b> command. Output fields are listed in the approximate order in which they appear.

**Table 242: show services rpm probe-results Output Fields**

Field Name	Field Description
<b>Owner</b>	Owner name. When you configure the probe owner statement at the <b>[edit services rpm]</b> hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is <b>Rpm-Bgp-Owner</b> .
<b>Test</b>	Name of a test representing a collection of probes. When you configure the test test-name statement at the <b>[edit services rpm probe owner]</b> hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is <b>Rpm-BGP-Test-<i>n</i></b> , where <i>n</i> is a cumulative number.
<b>Target address</b>	Destination address used for the probes.
<b>Source address</b>	Source address used for the probes.
<b>Probe type</b>	Protocol configured on the receiving probe server: <b>http-get</b> , <b>http-metadata-get</b> , <b>icmp-ping</b> , <b>icmp-ping-timestamp</b> , <b>tcp-ping</b> , <b>udp-ping</b> , or <b>udp-ping-timestamp</b> .
<b>Test size</b>	Number of probes within a test.

Table 242: show services rpm probe-results Output Fields (*continued*)

Field Name	Field Description
<b>Routing Instance Name</b>	<p>(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured:</p> <ul style="list-style-type: none"> <li>When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash ( / ) is used to separate the two entities. For example, if the routing instance called <b>R1</b> is configured within the logical system called <b>LS</b>, the name in the output field is <b>LS/R1</b>.</li> <li>When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance.</li> <li>When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by <b>default</b>. A slash ( / ) is used to separate the two entities. For example, <b>LS/default</b>.</li> </ul>
<b>Probe results</b>	<p>Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:</p> <ul style="list-style-type: none"> <li><b>Response received</b>—Timestamp when the probe result was determined.</li> <li><b>Client and server hardware timestamps</b>—If timestamps are configured, an entry appears at this point.</li> <li><b>Rtt</b>—Average ping round-trip time (RTT), in microseconds.</li> <li><b>Egress jitter</b>—Egress jitter, in microseconds.</li> <li><b>Ingress jitter</b>—Ingress jitter, in microseconds.</li> <li><b>Round trip jitter</b>—Round-trip jitter, in microseconds.</li> <li><b>Egress interarrival jitter</b>—Egress interarrival jitter, in microseconds.</li> <li><b>Ingress interarrival jitter</b>—Ingress interarrival jitter, in microseconds.</li> <li><b>Round trip interarrival jitter</b>—Round-trip interarrival jitter, in microseconds.</li> </ul>
<b>Results over current test</b>	<p>Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes.</p> <ul style="list-style-type: none"> <li><b>Probes sent</b>—Number of probes sent within the current test.</li> <li><b>Probes received</b>—Number of probe responses received within the current test.</li> <li><b>Loss percentage</b>—Percentage of lost probes for the current test.</li> <li><b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li><b>Samples</b>—Number of probes.</li> <li><b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li><b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li><b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li><b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li><b>Stddev</b>—Standard deviation, in microseconds.</li> <li><b>Sum</b>—Statistical sum.</li> </ul>

Table 242: show services rpm probe-results Output Fields (*continued*)

Field Name	Field Description
<b>Results over last test</b>	<p>Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent for the most recently completed test.</li> <li>• <b>Probes received</b>—Number of probe responses received for the most recently completed test.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes for the most recently completed test.</li> <li>• <b>Test completed</b>—Time the most recent test was completed.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul>
<b>Results over all tests</b>	<p>Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent in all tests.</li> <li>• <b>Probes received</b>—Number of probe responses received in all tests.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes in all tests.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types <b>icmp-ping-timestamp</b> and <b>udp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul>

## Sample Output

### show services rpm probe-results

```
user@host> show services rpm probe-results
```

```
Owner: probe_a, Test: a1
Target address: 200.1.1.2, Probe type: icmp-ping
Destination interface name: ge-0/0/6.0
Test size: 10 probes
Probe results:
 Response received, Sat Jul 30 11:52:21 2011, No hardware timestamps
 Rtt: 1897 usec
Results over current test:
 Probes sent: 8, Probes received: 8, Loss percentage: 0
 Measurement: Round trip time
 Samples: 8, Minimum: 1897 usec, Maximum: 7205 usec, Average: 2848 usec,
 Peak to peak: 5308 usec, Stddev: 1715 usec, Sum: 22783 usec
Results over last test:
 Probes sent: 10, Probes received: 10, Loss percentage: 0
 Test completed on Sat Jul 30 11:52:01 2011
 Measurement: Round trip time
 Samples: 10, Minimum: 1907 usec, Maximum: 8201 usec, Average: 3111 usec,
 Peak to peak: 6294 usec, Stddev: 2306 usec, Sum: 31106 usec
Results over all tests:
 Probes sent: 598, Probes received: 327, Loss percentage: 45
 Measurement: Round trip time
 Samples: 327, Minimum: 1878 usec, Maximum: 133729 usec,
 Average: 3304 usec, Peak to peak: 131851 usec, Stddev: 7561 usec,
 Sum: 1080434 usec
```

## 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 1711</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
```

## traceroute

**List of Syntax** [Syntax on page 1712](#)  
[Syntax \(QFX Series\) on page 1712](#)

**Syntax** `traceroute host`  
`<as-number-lookup>`  
`<bypass-routing>`  
`<clns>`  
`<gateway address>`  
`<inet | inet6>`  
`<interface interface-name>`  
`<logical system (all | logical-system-name)>`  
`<mpls (ldp FEC address | rsvp label-switched-path-name)>`  
`<no-resolve>`  
`<propagate-ttl>`  
`<routing-instance routing-instance-name>`  
`<source source-address>`  
`<tos value>`  
`<ttl value>`  
`<wait seconds>`

**Syntax (QFX Series)** `traceroute host`  
`<as-number-lookup>`  
`<bypass-routing>`  
`<gateway address>`  
`<inet>`  
`<interface interface-name>`  
`<monitor host>`  
`<no-resolve>`  
`<routing-instance routing-instance-name>`  
`<source source-address>`  
`<tos value>`  
`<ttl value>`  
`<wait seconds>`

**Release Information** Command introduced before Junos OS Release 7.4.  
 Command introduced in Junos OS Release 9.0 for EX Series switches.  
**mpls** option introduced in Junos OS Release 9.2.  
**propagate-ttl** option introduced in Junos OS Release 12.1.  
 Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description** Display the route that packets take to a specified network host. Use **traceroute** as a debugging tool to locate points of failure in a network.

**Options** **host**—IP address or name of remote host.

**as-number-lookup**—(Optional) Display the autonomous system (AS) number of each intermediate hop on the path from the host to the destination.

**bypass-routing**—(Optional) Bypass the normal routing tables and send requests directly to a system on an attached network. If the system is not on a directly attached

network, an error is returned. Use this option to display a route to a local system through an interface that has no route through it.

**clns**—(Optional) Trace the route belonging to Connectionless Network Service (CLNS).

**gateway address**—(Optional) Address of a router or switch through which the route transits.

**inet | inet6**—(Optional) Trace the route belonging to IPv4 or IPv6, respectively.

**interface interface-name**—(Optional) Name of the interface over which to send packets.

**logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**monitor host**—(Optional) Display real-time monitoring information for the specified host.

**monitor host**—(Optional) Perform this operation to display real-time monitoring information.

**monitor host**—(Optional) Perform this operation to display real-time monitoring information.

**mpls (ldp FEC address | rsvp label-switched-path name)**—(Optional).

**no-resolve**—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

**propagate-ttl**—(Optional) On the PE router, use this option to view locally-generated Routing Engine transit traffic. This is applicable for MPLS L3VPN traffic only. Use for troubleshooting, when you want to view hop-by-hop information from the local provider router to the remote provider router, when TTL decrementing is disabled on the core network using the **no-propagate-ttl** configuration statement.



**NOTE:** Using **propagate-ttl** with **traceroute** on the CE router does not show hop-by-hop information.

**routing-instance routing-instance-name**—(Optional) Name of the routing instance for the traceroute attempt.

**source source-address**—(Optional) Source address of the outgoing traceroute packets.

**tos value**—(Optional) Value to include in the IP type-of-service (ToS) field. The range of values is 0 through 255.

**ttl value**—(Optional) Maximum time-to-live value to include in the traceroute request. The range of values is 0 through 128.

**wait seconds**—(Optional) Maximum time to wait for a response to the traceroute request.

**Required Privilege Level** network

**List of Sample Output** [traceroute on page 1714](#)  
[traceroute as-number-lookup host on page 1714](#)  
[traceroute no-resolve on page 1714](#)  
[traceroute propagate-ttl on page 1715](#)  
[traceroute \(Between CE Routers, Layer 3 VPN\) on page 1715](#)  
[traceroute \(Through an MPLS LSP\) on page 1715](#)

**Output Fields** [Table 243 on page 1714](#) describes the output fields for the **traceroute** command. Output fields are listed in the approximate order in which they appear.

**Table 243: traceroute Output Fields**

Field Name	Field Description
<b>traceroute to</b>	IP address of the receiver.
<b>hops max</b>	Maximum number of hops allowed.
<b>byte packets</b>	Size of packets being sent.
<i>number-of-hops</i>	Number of hops from the source to the named router or switch.
<i>router-name</i>	Name of the router or switch for this hop.
<i>address</i>	Address of the router or switch for this hop.
<b>Round trip time</b>	Average round-trip time, in milliseconds (ms).

## Sample Output

### traceroute

```
user@host> traceroute santacruz
traceroute to host1.example.com (10.156.169.254), 30 hops max, 40 byte packets
 1 blue23 (10.168.1.254) 2.370 ms 2.853 ms 0.367 ms
 2 red14 (10.168.255.250) 0.778 ms 2.937 ms 0.446 ms
 3 yellow (10.156.169.254) 7.737 ms 89.905 ms 0.834 ms
```

### traceroute as-number-lookup host

```
user@host> traceroute as-number-lookup 10.100.1.1
traceroute to 10.100.1.1 (10.100.1.1), 30 hops max, 40 byte packets
 1 10.39.1.1 (10.39.1.1) 0.779 ms 0.728 ms 0.562 ms
 2 10.39.1.6 (10.39.1.6) [AS 32] 0.657 ms 0.611 ms 0.617 ms
 3 10.100.1.1 (10.100.1.1) [AS 10, 40, 50] 0.880 ms 0.808 ms 0.774 ms
```

### traceroute no-resolve

```
user@host> traceroute santacruz no-resolve
```



```

traceroute to host1.example.com (10.156.169.254), 30 hops max, 40 byte packets
 1 10.168.1.254 0.458 ms 0.370 ms 0.365 ms
 2 10.168.255.250 0.474 ms 0.450 ms 0.444 ms
 3 10.156.169.254 0.931 ms 0.876 ms 0.862 ms

```

#### traceroute propagate-ttl

```

user@host> traceroute propagate-ttl 100.200.2.2 routing-instance VPN-A
traceroute to 100.200.2.2 (100.200.2.2) from 1.1.0.2, 30 hops max, 40 byte packets

 1 1.2.0.2 (1.2.0.2) 2.456 ms 1.753 ms 1.672 ms
 MPLS Label=299776 CoS=0 TTL=1 S=0
 MPLS Label=299792 CoS=0 TTL=1 S=1
 2 1.3.0.2 (1.3.0.2) 1.213 ms 1.225 ms 1.166 ms
 MPLS Label=299792 CoS=0 TTL=1 S=1
 3 100.200.2.2 (100.200.2.2) 1.422 ms 1.521 ms 1.443 ms

```

#### traceroute (Between CE Routers, Layer 3 VPN)

```

user@host> traceroute vpn09
traceroute to host2.example.com (10.255.14.179), 30 hops max, 40
byte packets
 1 10.39.10.21 (10.39.10.21) 0.598 ms 0.500 ms 0.461 ms
 2 10.39.1.13 (10.39.1.13) 0.796 ms 0.775 ms 0.806 ms
 MPLS Label=100006 CoS=0 TTL=1 S=1
 3 host2.example.com (10.255.14.179) 0.783 ms 0.716 ms 0.686

```

#### traceroute (Through an MPLS LSP)

```

user@host> traceroute mpls1
traceroute to 10.168.1.224 (10.168.1.224), 30 hops max, 40 byte packets
 1 mpls1-sr0.company.net (10.168.200.101) 0.555 ms 0.393 ms 0.367 ms
 MPLS Label=1024 CoS=0 TTL=1
 2 mpls5-lo0.company.net (10.168.1.224) 0.420 ms 0.394 ms 0.401 ms

```



## CHAPTER 35

# System Log Monitoring and Troubleshooting Guide for Security Devices

- [Junos OS System Logging on page 1717](#)
- [Security Logging on page 1722](#)
- [Configuration Statements and Operational Commands on page 1751](#)

### Junos OS System Logging

---

- [Introduction to System Logging on page 1717](#)

#### Introduction to System Logging

- [Junos OS System Log Overview on page 1717](#)
- [Junos OS System Logging Facilities and Message Severity Levels on page 1718](#)
- [Junos OS Minimum System Logging Configuration on page 1719](#)
- [Junos OS Default System Log Settings on page 1720](#)
- [Junos OS Platform-Specific Default System Log Messages on page 1721](#)

#### Junos OS System Log Overview

---

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the device, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the *Junos OS System Log Reference*.



**NOTE:** This topic describes system log messages for Junos OS processes and libraries and not the system logging services on a Physical Interface Card (PIC) such as the Adaptive Services PIC.

#### Related Documentation

- [Junos OS System Log Configuration Hierarchy](#)
- [Junos OS Minimum System Logging Configuration on page 1719](#)

### Junos OS System Logging Facilities and Message Severity Levels

Table 244 on page 1718 lists the Junos system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

**Table 244: Junos OS System Logging Facilities**

Facility	Type of Event or Error
<b>any</b>	All (messages from all facilities)
<b>authorization</b>	Authentication and authorization attempts
<b>change-log</b>	Changes to the Junos OS configuration
<b>conflict-log</b>	Specified configuration is invalid on the router type
<b>daemon</b>	Actions performed or errors encountered by system processes
<b>dfc</b>	Events related to dynamic flow capture
<b>firewall</b>	Packet filtering actions performed by a firewall filter
<b>ftp</b>	Actions performed or errors encountered by the FTP process
<b>interactive-commands</b>	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
<b>kernel</b>	Actions performed or errors encountered by the Junos OS kernel
<b>pfe</b>	Actions performed or errors encountered by the Packet Forwarding Engine
<b>user</b>	Actions performed or errors encountered by user-space processes

Table 245 on page 1719 lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see [“Disabling the System Logging of a Facility” on page 1730](#).

**Table 245: System Log Message Severity Levels**

Severity Level	Description
<b>any</b>	Includes all severity levels
<b>none</b>	Disables logging of the associated facility to a destination
<b>emergency</b>	System panic or other condition that causes the router to stop functioning
<b>alert</b>	Conditions that require immediate correction, such as a corrupted system database
<b>critical</b>	Critical conditions, such as hard errors
<b>error</b>	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
<b>warning</b>	Conditions that warrant monitoring
<b>notice</b>	Conditions that are not errors but might warrant special handling
<b>info</b>	Events or nonerror conditions of interest

**Related Documentation**

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Junos OS Minimum System Logging Configuration

To record or view system log messages, you must include the **syslog** statement at the **[edit system]** hierarchy level. Specify at least one destination for the messages, as described in [Table 246 on page 1719](#). For more information about the configuration statements, see *Single-Chassis System Logging Configuration Overview*.

**Table 246: Minimum Configuration Statements for System Logging**

Destination	Minimum Configuration Statements
File	<pre>[edit system syslog] file filename {   facility severity; }</pre>
Terminal session of one, several, or all users	<pre>[edit system syslog] user (username   *) {   facility severity; }</pre>

**Table 246: Minimum Configuration Statements for System Logging (*continued*)**

Destination	Minimum Configuration Statements
Router or switch console	<code>[edit system syslog] console {   facility severity; }</code>
Remote machine or the other Routing Engine on the router or switch	<code>[edit system syslog] host (hostname   other-routing-engine) {   facility severity; }</code>

- Related Documentation**
- [Junos OS System Log Overview on page 1717](#)
  - [Overview of Junos OS System Log Messages](#)

### Junos OS Default System Log Settings

[Table 247 on page 1720](#) summarizes the default system log settings that apply to all routers that run the Junos OS, and specifies which statement to include in the configuration to override the default value.

**Table 247: Default System Logging Settings**

Setting	Default	Overriding Statement	Instructions
Alternative facility for message forwarded to a remote machine	For <b>change-log</b> : local6  For <b>conflict-log</b> : local5  For <b>dfc</b> : local1  For <b>firewall</b> : local3  For <b>interactive-commands</b> : local7  For <b>pfe</b> : local4	<code>[edit system syslog] host hostname {   facility-overrides facility; }</code>	<i>Changing the Alternative Facility Name for Remote System Log Messages</i>
Format of messages logged to a file	Standard Junos format, based on UNIX format	<code>[edit system syslog] file filename {   structured-data; }</code>	<a href="#">“Logging Messages in Structured-Data Format” on page 1724</a>
Maximum number of files in the archived set	10	<code>[edit system syslog] archive {   files number; } file filename {   archive {     files number;   } }</code>	<i>Specifying Log File Size, Number, and Archiving Properties</i>

Table 247: Default System Logging Settings (*continued*)

Setting	Default	Overriding Statement	Instructions
Maximum size of the log file	M Series, MX Series, and T Series: 1 megabyte (MB)  TX Matrix: 10 MB	<pre>[edit system syslog] archive {   size size; } file filename {   archive {     size size;   } }</pre>	<i>Specifying Log File Size, Number, and Archiving Properties</i>
Timestamp format	Month, date, hour, minute, second  For example: <b>Aug 21 12:36:30</b>	<pre>[edit system syslog] time-format format;</pre>	<i>"Including the Year or Millisecond in Timestamps" on page 1727</i>
Users who can read log files	<b>root</b> user and users with the Junos <b>maintenance</b> permission	<pre>[edit system syslog] archive {   world-readable; } file filename {   archive {     world-readable;   } }</pre>	<i>Specifying Log File Size, Number, and Archiving Properties</i>

- [Junos OS System Log Overview on page 1717](#)
- [Junos OS Platform-Specific Default System Log Messages on page 1721](#)

### Junos OS Platform-Specific Default System Log Messages

The following messages are generated by default on specific routers. To view any of these types of messages, you must configure at least one destination for messages as described in "[Junos OS Minimum System Logging Configuration](#)" on page 1719.

- To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

```
[edit system syslog]
(console | file filename | host destination | user username) {
 kernel info;
}
```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards all messages with a severity of **info** and higher to the master Routing Engine on the TX Matrix router. This is equivalent to the following configuration statement included on the TX Matrix router:

```
[edit system syslog]
host scc-master {
 any info;
}
```

- Likewise, on a routing matrix composed of a TX Matrix Plus router and T1600 routers, the master Routing Engine on each T1600 router forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

```
[edit system syslog]
host sfc0-master {
 any info;
}
```

**Related  
Documentation**

- [Junos OS System Log Overview on page 1717](#)
- [Junos OS Default System Log Settings on page 1720](#)

---

## Security Logging

- [Configuring System Logging for a Single-Chassis System on page 1722](#)
- [Directing System Log Messages to a Remote Destination on page 1732](#)
- [Displaying System Log Files on page 1734](#)
- [Displaying and Interpreting System Log Message Descriptions on page 1735](#)
- [Configuring System Logging for a Security Device on page 1744](#)

### Configuring System Logging for a Single-Chassis System

- [Specifying the Facility and Severity of Messages to Include in the Log on page 1722](#)
- [Directing System Log Messages to a Log File on page 1723](#)
- [Logging Messages in Structured-Data Format on page 1724](#)
- [Directing System Log Messages to a User Terminal on page 1724](#)
- [Directing System Log Messages to the Console on page 1725](#)
- [Including Priority Information in System Log Messages on page 1725](#)
- [System Log Default Facilities for Messages Directed to a Remote Destination on page 1726](#)
- [Including the Year or Millisecond in Timestamps on page 1727](#)
- [Using Regular Expressions to Refine the Set of Logged Messages on page 1728](#)
- [Disabling the System Logging of a Facility on page 1730](#)
- [Examples: Configuring System Logging on page 1730](#)

---

#### Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a *facility*, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions.



When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level or higher are logged to the destination:

```
[edit system syslog]
(console | file filename | host destination | user username) {
 facility severity;
}
```

**Related Documentation**

- [Junos OS System Logging Facilities and Message Severity Levels on page 1718](#)
- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Directing System Log Messages to a Log File

To direct system log messages to a file in the `/var/log` directory of the local Routing Engine, include the **file** statement at the `[edit system syslog]` hierarchy level:

```
[edit system syslog]
file filename {
 facility severity;
 archive <archive-sites (ftp-url <password password>)> <files number> <size size>
 <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
 no-world-readable>;
 explicit-priority;
 match "regular-expression";
 structured-data {
 brief;
 }
}
```

For the list of facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*.

To prevent log files from growing too large, the Junos OS system logging utility by default writes messages to a sequence of files of a defined size. By including the **archive** statement, you can configure the number of files, their maximum size, and who can read them, either for all log files or for a certain log file. For more information, see *Specifying Log File Size, Number, and Archiving Properties*.

For information about the following statements, see the indicated sections:

- **explicit-priority**—See “Including Priority Information in System Log Messages” on page 1725
- **match**—See “Using Regular Expressions to Refine the Set of Logged Messages” on page 1728
- **structured-data**—See “Logging Messages in Structured-Data Format” on page 1724

**Related Documentation**

- [Single-Chassis System Logging Configuration Overview](#)
- [Overview of Junos OS System Log Messages](#)
- [Logging Messages in Structured-Data Format on page 1724](#)

- [Examples: Configuring System Logging on page 1730](#)

### Logging Messages in Structured-Data Format

You can log messages to a file in structured-data format instead of the standard Junos format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol*, which is at <http://tools.ietf.org/html/draft-ietf-syslog-protocol-23>. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the **structured-data** statement at the **[edit system syslog file filename]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
 brief;
}
```

The optional **brief** statement suppresses the English-language text that appears by default at the end of a message to describe the error or event. For information about the fields in a structured-data format message, see the [System Log Explorer](#).

The structured format is used for all messages logged to the file that are generated by a Junos process or software library.



**NOTE:** If you include either or both of the explicit-priority and time-format statements along with the structured-data statement, they are ignored. These statements apply to the standard Junos system log format, not to structured-data format.

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Directing System Log Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the **user** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
user (username | *) {
 facility severity;
 match "regular-expression";
}
```

Specify one or more Junos OS usernames, separating multiple values with spaces, or use the asterisk (\*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*. For information about the **match** statement, see “[Using Regular Expressions to Refine the Set of Logged Messages](#)” on page 1728.

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Directing System Log Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the **console** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
 console {
 facility severity;
 }
```

For the list of logging facilities and severity levels, see *Specifying the Facility and Severity of Messages to Include in the Log*.

**Related  
Documentation**

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the **[edit system syslog file filename]** hierarchy level:

```
[edit system syslog file filename]
 facility severity;
 explicit-priority;
```



**NOTE:** Messages logged in structured-data format include priority information by default. If you include the **structured-data** statement at the **[edit system syslog file filename]** hierarchy level along with the **explicit-priority** statement, the **explicit-priority** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see “[Logging Messages in Structured-Data Format](#)” on page 1724. For information about the contents of a structured-data message, see the [System Log Explorer](#).

To include priority information in messages directed to a remote machine or the other Routing Engine, include the **explicit-priority** statement at the **[edit system syslog host (*hostname* | other-routing-engine)]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
 facility severity;
 explicit-priority;
```



**NOTE:** The **other-routing-engine** option does not apply to the QFX Series.

The priority recorded in a message always indicates the original, local facility name. If the **facility-override** statement is included for messages directed to a remote destination, the Junos OS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see *Changing the Alternative Facility Name for Remote System Log Messages*.

When the **explicit-priority** statement is included, the Junos OS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

*FACILITY-severity*[-TAG]

(The tag is a unique identifier assigned to some Junos OS system log messages; for more information, see the [System Log Explorer](#).)

In the following example, the **CHASSISD\_PARSE\_COMPLETE** message belongs to the **daemon** facility and is assigned severity **info (6)**:

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE:
 Using new configuration
```

When the **explicit-priority** statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new
 configuration
```

For more information about message formatting, see the [System Log Explorer](#).

#### Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- [Examples: Configuring System Logging on page 1730](#)

#### System Log Default Facilities for Messages Directed to a Remote Destination

[Table 248 on page 1727](#) lists the default alternative facility name next to the Junos OS-specific facility name for which it is used. For facilities that are not listed, the default alternative name is the same as the local facility name.

**Table 248: Default Facilities for Messages Directed to a Remote Destination**

Junos OS—specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3
interactive-commands	local7
pfe	local4

**Related Documentation**

- *Single-Chassis System Logging Configuration Overview*

**Including the Year or Millisecond in Timestamps**

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

Aug 21 12:36:30

To include the year, the millisecond, or both in the timestamp, include the **time-format** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

The modified timestamp is used in messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

The following example illustrates the format for a timestamp that includes both the millisecond (**401**) and the year (**2006**):

Aug 21 12:36:30.401 2006



**NOTE:** Messages logged in structured-data format include the year and millisecond by default. If you include the structured-data statement at the [edit system syslog file *filename*] hierarchy level along with the time-format statement, the time-format statement is ignored and messages are logged in structured-data format.

For information about the structured-data statement, see “[Logging Messages in Structured-Data Format](#)” on page 1724. For information about the contents of a structured-data message, see the [System Log Explorer](#).

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1730](#)

### Using Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

To specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the **match** statement and specify the regular expression which the text string must match:

```
match "regular-expression";
```

You can include this statement at the following hierarchy levels:

- [edit system syslog file *filename*] (for a file)
- [edit system syslog user (*username* | \*)] (for a specific user session or for all user sessions on a terminal)
- [edit system syslog host (*hostname* | other-routing-engine)] (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, <http://www.ieee.org>).

[Table 249 on page 1729](#) specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term *term* refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.



**NOTE:** The match statement is not case-sensitive.

Table 249: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
(pipe)	One of the terms that appears on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS-specific.
^ (caret)	Start of a line, when the caret appears outside square brackets.  One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
\$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen ( - ) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

**Using Regular Expressions**

Filter messages that belong to the **interactive-commands** facility, directing those that include the string **configure** to the terminal of the root user:

```
[edit system syslog]
user root {
 interactive-commands any;
 match ".*configure.*";
}
```

Messages like the following appear on the **root** user's terminal when a user issues a **configure** command to enter configuration mode:

```
timestamp router-name mgd[PID]: UI_CMDLINE_READ_LINE: User 'user', command
'configure private'
```

Filter messages that belong to the **daemon** facility and have a severity of **error** or higher, directing them to the file **/var/log/process-errors**. Omit messages generated by the SNMP process (snmpd), instead directing them to the file **/var/log/snmpd-errors**:

```
[edit system syslog]
file process-errors {
 daemon error;
```

```

match "!(.*snmpd.*)";
}
file snmpd-errors {
 daemon error;
 match ".*snmpd.*";
}

```

- Related Documentation**
- [Single-Chassis System Logging Configuration Overview](#)
  - [Examples: Configuring System Logging on page 1730](#)

### Disabling the System Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the **facility none** statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the **any severity** statement and then a **facility none** statement for each facility that you do not want to log. For example, the following logs all messages at the **error** level or higher to the console, except for messages from the **daemon** and **kernel** facilities. Messages from those facilities are logged to the file `>/var/log/internals` instead:

```

[edit system syslog]
console {
 any error;
 daemon none;
 kernel none;
}
file internals {
 daemon info;
 kernel info;
}

```

- Related Documentation**
- [Single-Chassis System Logging Configuration Overview](#)

### Examples: Configuring System Logging

The following example shows how to configure the logging of messages about all commands entered by users at the CLI prompt or invoked by client applications such as Junos XML protocol or NETCONF client applications, and all authentication or authorization attempts, both to the file **cli-commands** and to the terminal of any user who is logged in:

```

[edit system]
syslog {
 file cli-commands {
 interactive-commands info;
 authorization info;
 }
 user * {
 interactive-commands info;
 authorization info;
 }
}

```



```
}
```

The following example shows how to configure the logging of all changes in the state of alarms to the file `/var/log/alarms`:

```
[edit system]
syslog {
 file alarms {
 kernel warning;
 }
}
```

The following example shows how to configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user `alex`, to a remote machine, and to the console:

```
[edit system]
syslog {
 /* write all security-related messages to file /var/log/security */
 file security {
 authorization info;
 interactive-commands info;
 }
 /* write messages about potential problems to file /var/log/messages: */
 /* messages from "authorization" facility at level "notice" and above, */
 /* messages from all other facilities at level "warning" and above */
 file messages {
 authorization notice;
 any warning;
 }
 /* write all messages at level "critical" and above to terminal of user "alex" if */
 /* that user is logged in */
 user alex {
 any critical;
 }
 /* write all messages from the "daemon" facility at level "info" and above, and */
 /* messages from all other facilities at level "warning" and above, to the */
 /* machine monitor.mycompany.com */
 host monitor.mycompany.com {
 daemon info;
 any warning;
 }
 /* write all messages at level "error" and above to the system console */
 console {
 any error;
 }
}
```

The following example shows how to configure the handling of messages generated when users issue Junos OS CLI commands, by specifying the **interactive-commands** facility at the following severity levels:

- **info**—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file `/var/log/user-actions`.

- **notice**—Logs a message when users issue the configuration mode commands **rollback** and **commit**. The example writes the messages to the terminal of user **philip**.
- **warning**—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
 file user-actions {
 interactive-commands info;
 }
 user philip {
 interactive-commands notice;
 }
 console {
 interactive-commands warning;
 }
}
```

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)

## Directing System Log Messages to a Remote Destination

- [Adding a Text String to System Log Messages on page 1732](#)
- [Adding a String on page 1733](#)
- [Examples: Assigning an Alternative Facility on page 1733](#)

### Adding a Text String to System Log Messages

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the **log-prefix** statement at the **[edit system syslog host]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign ( = ) and the colon ( : ). It also cannot include the space character; do not enclose the string in quotation marks ( " ") in an attempt to include spaces in it.

The Junos OS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

The following example shows how to add the string **M120** to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine **hardware-logger.mycompany.com**:

```
[edit system syslog]
host hardware-logger.mycompany.com {
 any info;
 log-prefix M120;
```

```
}
```

When these configuration statements are included on an M120 router called **origin1**, a message in the system log on **hardware-logger.mycompany.com** looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user 'root', command 'run show version'
```

**Related Documentation**

- *Single-Chassis System Logging Configuration Overview*
- *Specifying Log File Size, Number, and Archiving Properties*

---

### Adding a String

Add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine **hardware-logger.mycompany.com**:

```
[edit system syslog]
host hardware-logger.mycompany.com {
 any info;
 log-prefix M120;
}
```

When these configuration statements are included on an M120 router called **origin1**, a message in the system log on **hardware-logger.mycompany.com** looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user 'root', command 'run show version'
```

---

### Examples: Assigning an Alternative Facility

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called **central-logger.mycompany.com**. The messages from California are assigned alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- Configure California routing platforms to aggregate messages in the **local0** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
 change-log info;
 facility-override local0;
}
```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

```
[edit system syslog]
host central-logger.mycompany.com {
```

```
change-log info;
facility-override local2;
}
```

On **central-logger**, you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

#### Related Documentation

- [Junos OS System Log Alternate Facilities for Remote Logging](#)

## Displaying System Log Files

- [Displaying a Log File from a Single-Chassis System on page 1734](#)
- [Examples: Displaying a Log File on page 1734](#)

### Displaying a Log File from a Single-Chassis System

---

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue either of the following commands:

```
user@host> show loglog-filename
user@host> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine. To display the file stored on a particular Routing Engine, prefix the file- or pathname with the string **re0** or **re1** and a colon. The following examples both display the **/var/log/messages** file stored on the Routing Engine in slot 1:

```
user@host> show log re1:messages
user@host> file show re1:/var/log/messages
```

For information about the fields in a log message, see *Interpreting Messages Generated in Standard Format by a Junos Process or Library*, “[Interpreting Messages Generated in Standard Format by Services on a PIC](#)” on page 1742, and “[Interpreting Messages Generated in Structured-Data Format](#)” on page 1737. For examples, see “[Examples: Displaying a Log File](#)” on page 1734.

### Examples: Displaying a Log File

---

Display the contents of the **/var/log/messages** file stored on the local Routing Engine. (The **/var/log** directory is the default location for log files, so you do not need to include it in the filename. The **messages** file is a commonly configured destination for system log messages.)

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]:
 UI_DBASE_LOGIN_EVENT: User 'barbara' entering configuration mode
Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara' exiting
 configuration mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no comment
Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82, ifAdminStatus
 up(1), ifOperStatus down(2), ifName at-1/0/0
```

Display the contents of the file `/var/log/processes`, which has been previously configured to include messages from the `daemon` facility. When issuing the `file show` command, you must specify the full pathname of the file:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
 SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
 trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
 SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
 SNMP trap: cold start
```

Display the contents of the file `/var/log/processes` when the `explicit-priority` statement is included at the `[edit system syslog file processes]` hierarchy level:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
start
Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared
all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

## Displaying and Interpreting System Log Message Descriptions

- [Displaying and Interpreting System Log Message Descriptions on page 1735](#)
- [Interpreting Messages Generated in Structured-Data Format on page 1737](#)
- [The message-source Field on a Single-Chassis System on page 1742](#)
- [Interpreting Messages Generated in Standard Format by Services on a PIC on page 1742](#)
- [Examples: Displaying System Log Message Descriptions on page 1743](#)

### Displaying and Interpreting System Log Message Descriptions

This reference lists the messages available at the time of its publication. To display the list of messages that applies to the version of the Junos OS that is running on a routing platform, enter Junos OS CLI operational mode and issue the following command:

```
user@host> help syslog ?
```

To display the list of available descriptions for tags whose names begin with a specific character string, substitute the string (in all capital letters) for the variable `TAG-PREFIX` (there is no space between the prefix and the question mark):

```
user@host> help syslog TAG-PREFIX?
```

To display the complete descriptions for tags whose name includes a regular expression, substitute a Perl-based expression for the variable `regex`. The match is not case-sensitive. For information about Perl-based regular expressions, consult a Perl reference manual or website such as <http://perldoc.perl.org>.

```
user@host> help syslog regex
```

To display the complete description of a particular message, substitute its name for the variable **TAG** (in all capital letters):

```
user@host> help syslog TAG
```

[Table 250 on page 1736](#) describes the fields in a system log message description in this reference or in the CLI.

**Table 250: Fields in System Log Message Descriptions**

Field Name in Reference	Field Name in CLI	Description
—	<b>Name</b>	The message tag in all capital letters.
<b>System Log Message</b>	<b>Message</b>	<p>Text of the message written to the system log. In the log, a specific value is substituted for each variable that appears in italics in this reference or in angle brackets (&lt; &gt;) in the CLI.</p> <p>In this reference, the message text appears on the second line of the <b>System Log Message</b> field. The first line is the message tag (the same text as in the CLI <b>Name</b> field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error.</p>
—	<b>Help</b>	Short description of the message, which also appears in the right-hand column of CLI output for the <b>help syslog</b> command when the output lists multiple messages.
<b>Description</b>	<b>Description</b>	More detailed explanation of the message.
<b>Type</b>	<b>Type</b>	<p>Category to which the message belongs:</p> <ul style="list-style-type: none"> <li>• <b>Error:</b> The message reports an error or failure condition that might require corrective action.</li> <li>• <b>Event:</b> The message reports a condition or occurrence that does not generally require corrective action.</li> </ul>

Table 250: Fields in System Log Message Descriptions (*continued*)

Field Name in Reference	Field Name in CLI	Description
Severity	Severity	Message severity level as described in Table: <b>System Log Message Severity Levels</b> in <i>Specifying the Facility and Severity of Messages to Include in the Log</i> .
Cause	Cause	(Optional) Possible cause for message generation. There can be more than one cause.
Action	Action	(Optional) Action you can perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.

### Interpreting Messages Generated in Structured-Data Format

Beginning in Junos OS Release 8.3, when the **structured-data** statement is included in the configuration for a log file, Junos processes and software libraries write messages to the file in structured-data format instead of the standard Junos format. For information about the **structured-data** statement, see [“Logging Messages in Structured-Data Format” on page 1724](#).

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values. In standard format, the variables are interspersed in the message text and not identified as variables.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

```
<priority code>version timestamp hostname process processID TAG [junos@2636.platform
variable-value-pairs] message-text
```

[Table 251 on page 1738](#) describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen ( - ) appears instead.

Table 251: Fields in Structured-Data Messages

Field	Description	Examples
<b>&lt;priority code&gt;</b>	Number that indicates the message's facility and severity. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see Table: <b>Facility and Severity Codes in the priority-code Field</b> in <i>Specifying the Facility and Severity of Messages to Include in the Log</i> .	<165> for a message from the <b>pfe</b> facility (facility=20) with severity <b>notice</b> (severity=5).
<b>version</b>	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version
<b>timestamp</b>	Time when the message was generated, in one of two representations: <ul style="list-style-type: none"> <li><b>YYYY-MM-DDTHH:MM:SS.MSZ</b> is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC)</li> <li><b>YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM</b> is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC</li> </ul>	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719-08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
<b>hostname</b>	Name of the host that originally generated the message.	router1
<b>process</b>	Name of the Junos process that generated the message.	mgd
<b>processID</b>	UNIX process ID (PID) of the Junos process that generated the message.	3046
<b>TAG</b>	Junos system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
<b>junos@2636.platform</b>	An identifier for the type of hardware platform that generated the message. The junos@2636 prefix indicates that the platform runs the Junos OS. It is followed by a dot-separated numerical identifier for the platform type. For a list of the identifiers, see <a href="#">Table 253 on page 1741</a> .	junos@2636.1.1.1.2.18 for the M120 router



Table 251: Fields in Structured-Data Messages (*continued*)

Field	Description	Examples
<i>variable-value-pairs</i>	A variable-value pair for each element in the <i>message-text</i> string that varies depending on the circumstances that triggered the message. Each pair appears in the format <i>variable = "value"</i> .	username="user"
<i>message-text</i>	English-language description of the event or error (omitted if the brief statement is included at the [edit system syslog file <i>filename</i> structured-data] hierarchy level). For the text for each message, see the chapters following System Log Messages.	User 'user' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="user"] User 'user' exiting configuration mode
```

When the brief statement is included at the [edit system syslog file *filename* structured-data ] hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="user"]
```

Table 252 on page 1739 maps the codes that appear in the *priority-code* field to facility and severity level.



**NOTE:** Not all of the facilities and severities listed in Table 252 on page 1739 can be included in statements at the [edit system syslog] hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see *Specifying the Facility and Severity of Messages to Include in the Log*.

Table 252: Facility and Severity Codes in the priority-code Field

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39

Table 252: Facility and Severity Codes in the priority-code Field (*continued*)

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103
security (13)	104	105	106	107	108	109	110	111
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Table 253 on page 1741 lists the numerical identifiers for routing platforms that appear in the **platform** field. The identifier is derived from the platform's SNMP object identifier (OID) as defined in the Juniper Networks routing platform MIB. For more information about OIDs, see the [Network Management Administration Guide for Routing Devices](#).

Table 253: Platform Identifiers in the platform Field

Identifier	Platform Name
1.1.1.2.1	M40 router
1.1.1.2.2	M20 router
1.1.1.2.3	M160 router
1.1.1.2.4	M10 router
1.1.1.2.5	M5 router
1.1.1.2.6	T640 routing node
1.1.1.2.7	T320 router
1.1.1.2.8	M40e router
1.1.1.2.9	M320 router
1.1.1.2.10	M7i router
1.1.1.2.11	M10i router
1.1.1.2.13	J2300 Services Router
1.1.1.2.14	J4300 Services Router
1.1.1.2.15	J6300 Services Router
1.1.1.2.17	TX Matrix platform
1.1.1.2.18	M120 router
1.1.1.2.19	J4350 Services Router
1.1.1.2.20	J6350 Services Router
1.1.1.2.23	J2320 Services Router
1.1.1.2.24	J2350 Services Router
1.1.1.2.27	T1600 router
1.1.1.2.83	T4000 router

### The message-source Field on a Single-Chassis System

The format of the **message-source** field in a message on a single-chassis system depends on whether the message was generated on the local Routing Engine or the other Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the **[edit system syslog host]** hierarchy level.

- When the local Routing Engine generated the message, there are two subfields:

*hostname process[process-ID]*

- When the other Routing Engine generated the message, there are three subfields:

*hostname reX process[process-ID]*

**hostname** is the hostname of the local Routing Engine.

**process[process-ID]** is the name and PID of the process that generated the message. If the **reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the **[process-ID]** part does not appear.

**reX** indicates that the other Routing Engine generated the message (**X** is **0** or **1**).

### Interpreting Messages Generated in Standard Format by Services on a PIC

Standard-format system log messages generated by services on a PIC, such as the Adaptive Services (AS) PIC, have the following syntax:

*timestamp (FPC Slot fpc-slot, PIC Slot pic-slot) {service-set} [SERVICE]:  
optional-string TAG: message-text*



**NOTE:** System logging for services on PICs is not configured at the **[edit system syslog]** hierarchy level as discussed in this chapter.

The (FPC Slot **fpc-slot**, PIC Slot **pic-slot**) field appears only when the standard system logging utility that runs on the Routing Engine writes the messages to the system log. When the PIC writes the message directly, the field does not appear.

Table 254 on page 1742 describes the message fields.

**Table 254: Fields in Messages Generated by a PIC**

Field	Description
<i>timestamp</i>	Time at which the message was logged.
<i>fpc-slot</i>	Slot number of the Flexible PIC Concentrator (FPC) that houses the PIC that generated the message.
<i>pic-slot</i>	Number of the PIC slot on the FPC in which the PIC that generated the message resides.

Table 254: Fields in Messages Generated by a PIC (*continued*)

Field	Description
<i>service-set</i>	Name of the service set that generated the message.
<i>SERVICE</i>	Code representing the service that generated the message. The codes include the following: <ul style="list-style-type: none"> <li>• FWNAT—Network Address Translation (NAT) service</li> <li>• IDS—Intrusion detection service</li> </ul>
<i>optional-string</i>	A text string that appears if the configuration for the PIC includes the log-prefix statement at the [edit interfaces interface-name services-options syslog] hierarchy level.
<i>TAG</i>	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating PIC. The entries in this reference are ordered alphabetically by this prefix.
<i>message-text</i>	Text of the message. For the text of each message, see System Log Messages.

### Examples: Displaying System Log Message Descriptions

Display the list of all currently available system log message descriptions:

```

user@host> help syslog ?

Possible completions:
<syslog-tag> Syslog tag
.
BOOTPD_ARG_ERR Command-line option was invalid
BOOTPD_BAD_ID Request failed because assembly ID was unknown
BOOTPD_BOOTSTRING tnp.bootpd provided boot string
BOOTPD_CONFIG_ERR tnp.bootpd could not parse configuration file;
 used default settings
BOOTPD_CONF_OPEN tnp.bootpd could not open configuration file
BOOTPD_DUP_REV Extra boot string definitions for revision were
 ignored
---(more 4%)---
```

Display the list of all currently available system log message descriptions for tags that begin with the letters **ACCT** (there is no space between **ACCT** and the question mark, and some descriptions are shortened for legibility):

```

user@host> help syslog ACCT?

Possible completions:
<syslog-tag> System log tag or regular expression
ACCT_ACCOUNTING_FERROR Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE Maximum file size is smaller than ...
ACCT_BAD_RECORD_FORMAT Record format does not match accounting profile
ACCT_CU_RTSLIB_ERROR Error occurred obtaining current class usage ...
ACCT_FORK_ERR Could not create child process
ACCT_FORK_LIMIT_EXCEEDED Could not create child process because of limit
ACCT_GETHOSTNAME_ERROR gethostname function failed
```

ACCT\_MALLOC\_FAILURE      Memory allocation failed  
ACCT\_UNDEFINED\_COUNTER\_NAME      Filter profile used undefined counter name  
ACCT\_XFER\_FAILED      Attempt to transfer file failed  
ACCT\_XFER\_POPEN\_FAIL      File transfer failed

Display the description of the `UI_CMDLINE_READ_LINE` message:

```
user@host> help syslog UI_CMDLINE_READ_LINE
```

```
Name: UI_CMDLINE_READ_LINE
Message: User '<users>', command '<input>'
Help: User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI
 prompt and pressed the Enter key, sending the command string
 to the management process (mgd).
Type: Event: This message reports an event, not an error
Severity: info
```

## Configuring System Logging for a Security Device

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Configuring Binary Security Log Files on page 1747](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

---

### Understanding System Logging for Security Devices

Junos OS supports configuring and monitoring of system log messages (also called *syslog messages*). You can configure files to log system messages and also assign attributes, such as severity levels, to messages. Reboot requests are recorded to the system log files, which you can view with the **show log** command.

This section contains the following topics:

- [Redundant System Log Server on page 1744](#)
- [Control Plane and Data Plane Logs on page 1745](#)

#### **Redundant System Log Server**

Security system logging traffic intended for remote servers is sent through the network interface ports, which support two simultaneous system log destinations. Each system logging destination must be configured separately. When two system log destination addresses are configured, identical logs are sent to both destinations. While two destinations can be configured on any device that supports the feature, adding a second destination is primarily useful as a redundant backup for standalone and active/backup configured chassis cluster deployments.

The following redundant server information is available:

- Facility: **cron**
- Description: cron scheduling process
- Severity Level (from highest to lowest severity): **debug**
- Description: Software debugging messages

### ***Control Plane and Data Plane Logs***

Junos OS generates separate log messages to record events that occur on the system's control and data planes.

- The control plane logs include events that occur on the routing platform. The system sends control plane events to the **eventd** process on the Routing Engine, which then handles the events by using Junos OS policies, by generating system log messages, or both. You can choose to send control plane logs to a file, user terminal, routing platform console, or remote machine. To generate control plane logs, use the **syslog** statement at the **[system]** hierarchy level.
- The data plane logs primarily include security events that the system has handled directly inside the data plane. These system logs are also referred to as *security logs*. How the system handles data plane events depends on the device:
  - For SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, the default logging mode is stream mode. The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine.

We recommend stream mode logging for the data plane. Data plane logs can be forwarded to the Routing Engine only when data plane logging is configured as an event mode.



**NOTE:** We recommend that only stream mode be used for security logs on high-end SRX Series devices. We do not recommend using event mode logging for high-end SRX Series devices. Supported logging rates apply to stream mode only. Logs might be dropped if you configure event mode logging on high-end SRX Series devices.

- For SRX100, SRX210, SRX220, SRX240, and SRX650 devices, by default, the system sends data plane events to the **eventd** process on the Routing Engine to be processed, formatted, and written to system log files in a similar manner to control plane events.

### **Related Documentation**

- [Understanding Binary Format for Security Logs on page 1746](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

## Understanding Binary Format for Security Logs

---

The Junos operating system (Junos OS) generates separate log messages to record events that occur on the system's control plane and data plane. The control plane monitors events that occur on the routing platform. Such events are recorded in system log messages. To generate system log messages, use the **syslog** statement at the **[system]** hierarchy level.

Data plane log messages, referred to as security log messages, record security events that the system handles directly inside the data plane. To generate security log messages, use the **log** statement at the **[security]** hierarchy level.

System log messages are maintained in log files in text-based formats, such as BSD Syslog, Structured Syslog, and WebTrends Enhanced Log Format (WELF).

Security log messages can also be maintained in text-based formats. Because security logging can produce large amounts of data, however, text-based log files can quickly consume storage and CPU resources. Depending on your implementation of security logging, a log file in a binary-based format can provide more efficient use of on-box or off-box storage and improved CPU utilization. Binary format for security log messages is available on all SRX Series devices.

When configured in event mode, security log messages generated in the data plane are directed to the control plane and stored locally on the device. Security log messages stored in binary format are maintained in a log file separate from that used to maintain system log messages. Events stored in a binary log file are not accessible with advanced log-scripting commands intended for text-based log files. A separate CLI operational command supports decoding, converting, and viewing binary log files that are stored locally on the device.

When configured in stream mode, security log messages generated in the data plane are streamed to a remote device. When these messages are stored in binary format, they are streamed directly to external log collection clients in a Juniper-specific binary format. The external client handles decoding, converting, and viewing binary log files that are stored on a remote device.

### Related Documentation

- [Configuring Binary Security Log Files on page 1747](#)
- [Understanding System Logging for Security Devices on page 1744](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)



### Configuring Binary Security Log Files

You can configure security files in binary format using the **log** statement at the **[security]** hierarchy level.

The following procedure specifies binary format for event-mode or stream-mode logging, and defines the log filename, path, and log file characteristics.

1. Specify the format for the log file.
  - For on-box, event-mode logging:
 

```
set security log mode event
set security log format binary
```
  - For off-box, stream-mode logging:
 

```
set security log mode stream
set security log stream test-stream format binary host 1.3.54.22
```
2. For off-box security logging, specify the source address, which identifies the SRX Series device that generated the log messages. The source address is required.
 

```
set security log source-address 2.3.45.66
```
3. Optionally, define a log filename and a path. By default, the file `bin_messages` is created in the `/var/log` directory.
 

```
set security log file name security-binary-log
set security log file path security/log-folder
```
4. Optionally, change the maximum size of the log file and the maximum number of log files that can be archived. By default, the maximum size of the log file is 3 MB, and a total of three log files can be archived.
 

```
set security log file size 5
set security log file files 5
```
5. Optionally, select the `hpl` flag to enable diagnostic traces for binary logging. The prefix `smf_hpl` identifies all binary logging traces.
 

```
set security log traceoptions flag hpl
```
6. View the content of the event-mode log file stored on the device.



**NOTE:** The `show security log` command displays event-mode security log messages if they are in a text-based format. The `show security log file` command displays event-mode security log messages if they are in binary format.

```
show security log file
```

Use the following command to clear the content of the binary event-mode security log file.

```
clear security log file
```



**NOTE:** Third-party tools decode and convert log files to binary text when they are streamed to a remote device. Refer to your third-party documentation for details about displaying streamed security log messages.

#### Related Documentation

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

#### Sending System Log Messages to a File

You can direct system log messages to a file on the CompactFlash (CF) card. The default directory for log files is `/var/log`. To specify a different directory on the CF card, include the complete pathname.

Create a file named **security**, and send log messages of the **authorization** class at the severity level **info** to the file.

To set the filename, the facility, and severity level:

```
{primary:node0}
user@host# set system syslog file security authorization info
```

#### Related Documentation

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

#### Setting the System to Send All Log Messages Through eventd

The **eventd** process of logging configuration is most commonly used for Junos OS. In this configuration, control plane logs and data plane, or security, logs are forwarded from the data plane to the Routing Engine control plane **rtlogd** process. The **rtlogd** process then either forwards syslog or sd-syslog-formatted logs to the **eventd** process or the WELF-formatted logs to the external or remote WELF log collector.

To send all log messages through **eventd**:

1. Set the **eventd** process to handle security logs and send them to a remote server.

```
{primary:node0}
user@host# set security log mode event
```

2. Configure the server that will receive the system log messages.

```
{primary:node0}
user@host# set system syslog host hostname any any
```

where *hostname* is the fully qualified hostname or IP address of the server that will receive the logs.



**NOTE:** To send duplicate logs to a second remote server, repeat the command with a new fully qualified *hostname* or IP address of a second server.

If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

To rename or redirect one of the logging configurations, you need to delete and recreate it. To delete a configuration:

```
{primary:node0}
user@host# delete security log mode event
```

#### Related Documentation

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1749](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

### Setting the System to Stream Security Logs Through Revenue Ports

You can increase the number of data plane, or security, logs that are sent by modifying the manner in which they are sent. When the logging mode is set to **stream**, security logs generated in the data plane are streamed out a revenue traffic port directly to a remote server.

To use the **stream** mode, enter the following commands:

```
{primary:node0}
user@host# set security log mode stream source-address source-address
user@host# set security log stream streamname format (syslog|sd-syslog|welf) category
(all|content-security) host ipaddr
```

where *source-address* is the IP address of the source machine; **syslog**, **sd-syslog** (structured system logging messages) and **welf** are logging formats; **all** and **content-security** are the categories of logging; and *ipaddr* is the IP address of the server to which the logs will be streamed.



**NOTE:** WELF logs must be streamed through a revenue port because the `eventd` process does not recognize the WELF format. The category must be set to `content-security`. For example:

```
{primary:node0}
user@host# set security log stream securitylog1 format welf category
content-security host 10.121.23.5
```

To send duplicate logs to a second remote server, repeat the command with a new *ipaddr*. If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

#### Related Documentation

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Setting the System to Send All Log Messages Through eventd on page 1748](#)
- [Sending System Log Messages to a File on page 1748](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1750](#)

### Monitoring System Log Messages with the J-Web Event Viewer

**Purpose** Monitor errors and events that occur on the device.

**Action** Select **Monitor>Events and Alarms>View Events** in the J-Web user interface.

The J-Web View Events page displays the following information about each event:

- **Process**—System process that generated the error or event.
- **Severity**—A severity level 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:
  - **Debug/Info/Notice (Green)**—Indicates conditions that are not errors but are of interest or might warrant special handling.
  - **Warning (Yellow)**—Indicates conditions that warrant monitoring.
  - **Error (Blue)**—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
  - **Critical (Pink)**—Indicates critical conditions, such as hard drive errors.
  - **Alert (Orange)**—Indicates conditions that require immediate correction, such as a corrupted system database.
  - **Emergency (Red)**—Indicates system panic or other conditions that cause the routing platform to stop functioning.
- **Event ID**—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.

To control which errors and events are displayed in the list, use the following options:

- System Log File—Specify the name of the system log file that records the errors and events.
- Process—Specify the system processes that generate the events you want to display. To view all the processes running on your system, enter the **show system processes** CLI command.
- Date From—Specify the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.
- To—Specify the end of the date range that you want to monitor. Set the date using the calendar pick tool.
- Event ID—Specify the specific ID of the error or event that you want 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.
- Generate Report—Creates an HTML report based on the specified parameters.

**Related  
Documentation**

- [Understanding System Logging for Security Devices on page 1744](#)
- [Understanding Binary Format for Security Logs on page 1746](#)
- [Monitoring Overview on page 1283](#)
- [Monitoring Interfaces on page 1400](#)

---

## Configuration Statements and Operational Commands

- [Configuration Statements on page 1751](#)
- [Operational Commands on page 1780](#)

### Configuration Statements

- [allow-duplicates on page 1753](#)
- [archive \(All System Log Files\) on page 1754](#)
- [cache \(Security Log\) on page 1755](#)
- [console \(System Logging\) on page 1756](#)
- [destination-override on page 1757](#)
- [event-rate on page 1757](#)
- [exclude \(Security Log\) on page 1758](#)
- [explicit-priority on page 1759](#)

- [facility-override](#) on page 1759
- [file \(Security Log\)](#) on page 1760
- [file \(System Logging\)](#) on page 1761
- [files](#) on page 1762
- [host \(Security Log\)](#) on page 1763
- [limit \(Security Log\)](#) on page 1763
- [log \(Services\)](#) on page 1764
- [log-prefix \(System\)](#) on page 1765
- [log-rotate-frequency](#) on page 1765
- [match](#) on page 1766
- [mode \(Security Log\)](#) on page 1766
- [no-remote-trace \(System\)](#) on page 1767
- [pic-services-logging](#) on page 1767
- [port](#) on page 1768
- [rate-cap](#) on page 1768
- [security-log](#) on page 1769
- [security-log-percent-full](#) on page 1770
- [severity \(Security Log\)](#) on page 1770
- [size](#) on page 1771
- [structured-data](#) on page 1772
- [syslog \(System\)](#) on page 1773
- [system](#) on page 1774
- [time-format](#) on page 1775
- [traceoptions \(Security Log\)](#) on page 1776
- [tracing](#) on page 1778
- [user \(System Logging\)](#) on page 1779
- [world-readable](#) on page 1780

## allow-duplicates

---

<b>Syntax</b>	allow-duplicates;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog], [edit logical-systems <i>logical-system-name</i> system syslog file <i>file-name</i> ], [edit logical-systems <i>logical-system-name</i> system syslog host <i>host-name</i> ], [edit logical-systems <i>logical-system-name</i> system syslog user <i>user-name</i> ], [edit system syslog], [edit system syslog file <i>file-name</i> ], [edit system syslog host <i>host-name</i> ], [edit system syslog user <i>user-name</i> ],
<b>Release Information</b>	Statement introduced in Release 11.1 of Junos OS. Logical systems support introduced in Release 11.4 of Junos OS.
<b>Description</b>	Specify whether to allow the repeated messages in the system log output files. This can be set either at global configuration level or for individual file, host, or user. By default, this parameter is set to disable.
<b>Options</b>	<b>file</b> —Name of the file to log messages  <b>host</b> —Host to receive the messages  <b>user</b> —User to receive the notification of the event
<b>Required Privilege Level</b>	<b>system</b> —To view this statement in the configuration. <b>system-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>

## archive (All System Log Files)

<b>Syntax</b>	<pre>archive &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;start-time <i>time</i>&gt; &lt;transfer-interval <i>interval</i>&gt;     &lt;binary-data   no-binary-data&gt;;     &lt;world-readable   no-world-readable&gt;;</pre>
<b>Hierarchy Level</b>	[edit system <a href="#">syslog</a> ]
<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>	Configure archiving properties for all system log files.
<b>Options</b>	<p><b>files <i>number</i></b>—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <b>logfile</b>, it closes the file, compresses it, and renames it <b>logfile.0.gz</b> (the amount of data is determined by the <b>size</b> statement at this hierarchy level). The utility then opens and writes to a new file called <b>logfile</b>. When the new file reaches the maximum size, the <b>logfile.0.gz</b> file is renamed to <b>logfile.1.gz</b>, and the new file is closed, compressed, and renamed <b>logfile.0.gz</b>. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).</p> <p><b>Range:</b> 1 through 1000</p> <p><b>Default:</b> 10 files</p> <p><b>size <i>size</i></b>—Maximum amount of data that the Junos OS logging utility writes to a log file <b>logfile</b> before archiving it (closing it, compressing it, and changing its name to <b>logfile.0.gz</b>). The utility then opens and writes to a new file called <b>logfile</b>.</p> <p><b>Syntax:</b> <i>x k</i> to specify the number of kilobytes, <i>x m</i> for the number of megabytes, or <i>x g</i> for the number of gigabytes</p> <p><b>Range:</b> 64 KB through 1 GB</p> <p><b>Default:</b></p> <ul style="list-style-type: none"> <li>• 128 KB for EX Series switches</li> <li>• 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch</li> <li>• 10 MB for TX Matrix and TX Matrix Plus routers</li> </ul> <p><b>binary-data   no-binary-data</b>—Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems)..</p> <p><b>Default:</b> no-binary-data</p> <p><b>world-readable   no-world-readable</b>—Grant all users permission to read archived log files, or restrict the permission only to the <b>root</b> user and users who have the Junos OS <b>maintenance</b> permission.</p> <p><b>Default:</b> no-world-readable</p>



**Required Privilege Level** system—To view this statement in the configuration.  
 system-control—To add this statement to the configuration.

**Related Documentation** • *Specifying Log File Size, Number, and Archiving Properties*

## cache (Security Log)

**Syntax**

```
cache {
 exclude exclude-name {
 destination-address destination-address;
 destination-port destination-port;
 event-id event-id;
 failure;
 interface-name interface-name;
 policy-name policy-name;
 process process-name;
 protocol protocol;
 source-address source-address;
 source-port source-address;
 success;
 user-name user-name;
 }
 limit value;
}
```

**Hierarchy Level** [edit security log]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Cache security log events in the audit log buffer.

**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** • [syslog \(System\) on page 1773](#)

## console (System Logging)

---

<b>Syntax</b>	<pre>console {     <i>facility severity</i>; }</pre>
<b>Hierarchy Level</b>	[edit system <a href="#">syslog</a> ]
<b>Release Information</b>	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 the logging of system messages to the system console.
<b>Options</b>	<p><b><i>facility</i></b>—Class of messages to log. To specify multiple classes, include multiple <b><i>facility severity</i></b> statements. For a list of the facilities, see <a href="#">Table 244 on page 1718</a>.</p> <p><b><i>severity</i></b>—Severity of the messages that belong to the facility specified by the paired <b><i>facility</i></b> name. Messages with severities of the specified level and higher are logged. For a list of the severities, see <a href="#">Table 245 on page 1719</a>.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Directing System Log Messages to the Console on page 1725</a></li></ul>

## destination-override

---

<b>Syntax</b>	destination-override { syslog host <i>ip-address</i> ; }
<b>Hierarchy Level</b>	[edit system tracing]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	This option overrides the system-wide configuration under <b>[edit system tracing]</b> and has no effect if system tracing is not configured.
<b>Options</b>	These options specify the system logs and the host to which remote tracing output is sent: <ul style="list-style-type: none"> <li>• <b>syslog</b>—Specify the system process log files to send to the remote tracing host.</li> <li>• <b>host <i>ip-address</i></b>—Specify the IP address to which to send tracing information.</li> </ul>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">tracing on page 1778</a></li> </ul>

## event-rate

---

<b>Syntax</b>	Syntax event-rate <i>rate</i>
<b>Hierarchy Level</b>	[edit security log]
<b>Release Information</b>	Statement introduced in Release 10.0 of Junos OS.
<b>Description</b>	Limits the rate (0 to 1500) at which logs will be streamed per second.
<b>Options</b>	The remaining statements are explained separately. See <a href="#">CLI Explorer</a> .
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>

## exclude (Security Log)

---

**Syntax**    `exclude exlude-name {  
                  destination-address destination-address;  
                  destination-port destination-port;  
                  event-id event-id;  
                  failure;  
                  interface-name interface-name;  
                  policy-name policy-name;  
                  process process-name;  
                  protocol protocol;  
                  source-address source-address;  
                  source-port source-port;  
                  success;  
                  user-name user-name;  
                  }`

**Hierarchy Level**    [edit security log cache]

**Release Information**    Statement introduced in Release 11.2 of Junos OS.

**Description**    Configure a list of auditable events that can be excluded from the audit log.

- Options**
- **destination-ip *destination-address***—Destination IP address.
  - **destination-port *destination-port***—Destination port number.
  - **event-id *event-id***—Error message identification number.
  - **failure**—Failed audit event logs.
  - **interface-name *interface-name***—Name of the interface.
  - **policy-name *policy-name***—Policy name filter.
  - **process *process-name***—Process that generated the event.
  - **protocol *protocol***—Protocol that generated the event.
  - **source-ip *source-address***—Source IP address.
  - **source-port *source-port***—Source port number.
  - **success**—Successful audit event logs.
  - **username *user-name***—User name filter.

**Required Privilege Level**    security—To view this statement in the configuration.  
                                  security-control—To add this statement to the configuration.

- Related Documentation**
- [show security log on page 1791](#)
  - [clear security log on page 1782](#)

## explicit-priority

<b>Syntax</b>	explicit-priority;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit logical-systems <i>logical-system-name</i> system syslog host], [edit system syslog file <i>filename</i> ], [edit system syslog host]
<b>Release Information</b>	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>	Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination.  When the <b>structured-data</b> statement is also included at the [edit system syslog file <i>filename</i> ] hierarchy level, this statement is ignored for the file.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Including Priority Information in System Log Messages on page 1725</a></li> <li>• <i>Junos OS System Log Reference</i></li> <li>• <a href="#">structured-data on page 1772</a></li> </ul>

## facility-override

<b>Syntax</b>	facility-override <i>facility</i> ;
<b>Hierarchy Level</b>	[edit system syslog host]
<b>Release Information</b>	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>	Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.
<b>Options</b>	<i>facility</i> —Alternate facility to substitute for the default facilities. For a list of the possible facilities, see <i>Junos OS System Log Alternate Facilities for Remote Logging</i> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Changing the Alternative Facility Name for Remote System Log Messages</i></li> <li>• <i>Junos OS System Log Reference</i></li> </ul>

## file (Security Log)

---

Syntax	<pre>file {     files <i>max-file-number</i>;     name <i>file-name</i>;     path <i>binary-log-file-path</i>;     size <i>maximum-file-size</i>; }</pre>
Hierarchy Level	[edit security log]
Release Information	Statement modified in Release 9.2 of Junos OS.
Description	Configure security log file options for logs in binary format.
Options	<ul style="list-style-type: none"><li>• <b>files <i>number</i></b>—Specify the maximum number of binary log files. <b>Range:</b> 2 through 10 files.</li><li>• <b>name <i>name</i></b> —Name of the file to log messages.</li><li>• <b>path <i>filepath</i></b>—Specify the path of the binary log file.</li><li>• <b>size <i>maximum-file-size</i></b>—Maximum size of each trace file, in megabytes (MB). <b>Range:</b> 1 KB through 10 MB</li></ul>
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"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>

## file (System Logging)

<b>Syntax</b>	<pre> file <i>filename</i> {     <i>facility severity</i>;     archive {         <i>files number</i>;         <i>size size</i>;         (no-world-readable   world-readable);     }     explicit-priority;     match "<i>regular-expression</i>";     structured-data {         brief;     } } </pre>
<b>Hierarchy Level</b>	[edit system <a href="#">syslog</a> ]
<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>	Configure the logging of system messages to a file.
<b>Options</b>	<p><b><i>facility</i></b>—Class of messages to log. To specify multiple classes, include multiple <b><i>facility severity</i></b> statements. For a list of the facilities, see <a href="#">Table 244 on page 1718</a>.</p> <p><b><i>file filename</i></b>—File in the <code>/var/log</code> directory in which to log messages from the specified facility. To log messages to more than one file, include more than one <b><i>file</i></b> statement.</p> <p><b><i>severity</i></b>—Severity of the messages that belong to the facility specified by the paired <b><i>facility</i></b> name. Messages with severities of the specified level and higher are logged. For a list of the severities, see <a href="#">Table 245 on page 1719</a>.</p> <p>The remaining statements are explained separately.</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Directing System Log Messages to a Log File on page 1723</a></li> <li>• <a href="#">Junos OS System Log Reference</a></li> </ul>


## files

---

<b>Syntax</b>	<code>files <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
<b>Release Information</b>	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 EX Series switches.
<b>Description</b>	Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file <i>logfile</i> , it closes the file, compresses it, and renames it to <i>logfile.0.gz</i> (for information about the maximum file size, see <a href="#">size</a> ). The utility then opens and writes to a new file called <i>logfile</i> . When the new file reaches the maximum size, the <i>logfile.0.gz</i> file is renamed to <i>logfile.1.gz</i> , and the new file is closed, compressed, and renamed <i>logfile.0.gz</i> . By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).
<b>Options</b>	<i>number</i> —Maximum number of archived files. <b>Range:</b> 1 through 1000 <b>Default:</b> 10 files
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Specifying Log File Size, Number, and Archiving Properties</i></li><li>• <i>Junos OS System Log Reference</i></li><li>• <a href="#">size on page 1771</a></li></ul>



## host (Security Log)

<b>Syntax</b>	host { <i>ip-address</i> ; port <i>port-number</i> ; }
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	You can specify the IP address of the server to which the security logs will be streamed.
<div>  <p><b>NOTE:</b> On SRX3400, SRX3600, SRX5600, and SRX5800 devices, if the stream configuration does not specify a destination port, the default destination port will be the syslog port. If you specify a destination port in the stream configuration, then that port will be used instead.</p> </div>	
<b>Options</b>	<ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specify the IP address of the host.</li> <li>• <i>port port-number</i>—Specify the UDP port number.</li> </ul>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>

## limit (Security Log)

<b>Syntax</b>	limit <i>value</i> ;
<b>Hierarchy Level</b>	[edit security log cache]
<b>Release Information</b>	Statement modified in Release 9.2 of Junos OS.
<b>Description</b>	Specify the number of security log entries to be kept in memory.
<b>Options</b>	Once the maximum value limit is reached, new entries will not be added until the cache size drops. <b>Range:</b> 0 through 4,294,967,295
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>

## log (Services)

---

<b>Syntax</b>	<pre>log {   all;   errors;   info;   sessions-allowed;   sessions-dropped;   sessions-ignored;   sessions-whitelisted;   warning; }</pre>
<b>Hierarchy Level</b>	[edit services ssl proxy profile <i>profile-name</i> actions]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D10.
<b>Description</b>	Specify the logging actions.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>all</b>—Log all events.</li><li>• <b>errors</b>—Log all error events.</li><li>• <b>info</b>—Log all information events.</li><li>• <b>sessions-allowed</b>—Log SSL session allowed events after an error.</li><li>• <b>sessions-dropped</b>—Log only SSL session dropped events.</li><li>• <b>sessions-ignored</b>—Log session ignored events.</li><li>• <b>sessions-whitelisted</b>—Log SSL session whitelisted events.</li><li>• <b>warning</b>—Log all warning events.</li></ul>
<b>Required Privilege Level</b>	services—To view this statement in the configuration. services-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring SSL Proxy</i></li></ul>

## log-prefix (System)

---

<b>Syntax</b>	<code>log-prefix <i>string</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog host]
<b>Release Information</b>	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>	Include a text string in each message directed to a remote destination.
<b>Options</b>	<i>string</i> —Text string to include in each message.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Adding a Text String to System Log Messages on page 1732</a></li><li>• <a href="#">System Log Explorer</a></li></ul>

## log-rotate-frequency

---

<b>Syntax</b>	<code>log-rotate-frequency <i>frequency</i>;</code>
<b>Hierarchy Level</b>	[set system <a href="#">syslog</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.3.
<b>Description</b>	Configure the system log file rotation frequency by configuring the time interval for checking the log file size.  When the log file size has exceeded the configured limit, the old log file is archived and a new log file is created.
<b>Options</b>	<i>frequency</i> —Frequency of rotation of the system log file. <b>Range:</b> 1 minute through 59 minutes <b>Default:</b> 15 minutes
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Specifying Log File Size, Number, and Archiving Properties</a></li><li>• <a href="#">syslog on page 1773</a></li></ul>

## match

---

<b>Syntax</b>	<code>match "regular-expression";</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit logical-systems <i>logical-system-name</i> system syslog user ( <i>username</i>   *)], [edit system syslog file <i>filename</i> ], [edit system syslog host <i>hostname</i>   other-routing-engine  scc-master)], [edit system syslog user ( <i>username</i>   *)]
<b>Release Information</b>	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>	Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Using Regular Expressions to Refine the Set of Logged Messages on page 1728</a></li></ul>

## mode (Security Log)

---

<b>Syntax</b>	<code>mode (event   stream)</code>
<b>Hierarchy Level</b>	[edit security log]
<b>Release Information</b>	Statement introduced in Release 10.0 of Junos OS.
<b>Description</b>	Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server).
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>event</b>—Process security logs in the control plane.</li><li>• <b>stream</b>—Process security logs directly in the forwarding plane.</li></ul> <p><b>Default:</b> event.</p>
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>

## no-remote-trace (System)

<b>Syntax</b>	no-remote-trace;
<b>Hierarchy Level</b>	[edit system scripts commit traceoptions]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Disable remote tracing.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">traceoptions (Security Datapath Debug) on page 1601</a></li> </ul>

## pic-services-logging

<b>Syntax</b>	<pre>pic-services-logging {   command <i>binary-file-path</i>;   disable;   failover (alternate-media   other-routing-engine); }</pre>
<b>Hierarchy Level</b>	[edit system processes]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Enable PICs to send special logging information to the Routing Engine for archiving on a hard disk.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>command <i>binary-file-path</i></b>—Path to the binary process.</li> <li>• <b>disable</b>—Disable the PIC services logging process.</li> <li>• <b>failover</b>—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"> <li>• <b>alternate-media</b>—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.</li> <li>• <b>other-routing-engine</b>—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, the device reboots from the secondary Routing Engine.</li> </ul> </li> </ul>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>

## port

---

<b>Syntax</b>	<code>port <i>port number</i>;</code>
<b>Hierarchy Level</b>	[edit system syslog host <i>hostname</i>   other-routing-engine  scc-master)]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.3.
<b>Description</b>	Specify the port number for the remote syslog server.
<b>Options</b>	<b><i>port number</i></b> —Port number of the remote syslog server. <b>Range:</b> 0 through 65535 <b>Default:</b> 514
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog on page 1773</a></li><li>• <i>host</i></li></ul>

## rate-cap

---

<b>Syntax</b>	<code>rate-cap <i>rate-cap-value</i>;</code>
<b>Hierarchy Level</b>	[edit security log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Limit the rate (0 to 5000) at which logs will be streamed per second. By default, the rate cap value is 100 logs per second.
<b>Required Privilege Level</b>	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog on page 1773</a></li></ul>

## security-log

---

Syntax	<pre>security-log {     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 security log process.
Options	<ul style="list-style-type: none"><li>• <b>command <i>binary-file-path</i></b>—Path to the binary process.</li><li>• <b>disable</b>—Disable the security log process.</li><li>• <b>failover</b>—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"><li>• <b>alternate-media</b>—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.</li><li>• <b>other-routing-engine</b>—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.</li></ul></li></ul>
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"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>

## security-log-percent-full

---

<b>Syntax</b>	<code>security-log-percent-full <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit security alarms potential-violation]
<b>Release Information</b>	Statement introduced in Release 11.2 of Junos OS.
<b>Description</b>	Raise a security alarm when security log exceeds a specified percent of total capacity.
<b>Options</b>	<b><i>percentage</i></b> —Percentage of security log capacity at which a security alarm is raised. <b>Range:</b> 0 through 100 percent
<b>Required Privilege Level</b>	<code>security</code> —To view this statement in the configuration. <code>security-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>

## severity (Security Log)

---

<b>Syntax</b>	<code>severity (alert   critical   debug   emergency   error   info   notice   warning)</code>
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement modified in Release 9.2 of Junos OS.
<b>Description</b>	Set severity threshold for security logs.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>alert</b>—Conditions that require immediate attention.</li><li>• <b>critical</b>—Critical conditions.</li><li>• <b>debug</b>—Information normally used in debugging.</li><li>• <b>emergency</b>—Conditions that cause security functions to stop.</li><li>• <b>error</b>—General error conditions.</li><li>• <b>info</b>—Information about normal security operations.</li><li>• <b>notice</b>—Nonerror conditions that are of interest.</li><li>• <b>warning</b>—General warning conditions.</li></ul> <b>Default:</b> debug.
<b>Required Privilege Level</b>	<code>security</code> —To view this statement in the configuration. <code>security-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>




## size

---

<b>Syntax</b>	<code>size size;</code>
<b>Hierarchy Level</b>	[edit system syslog archive], [edit system syslog file <i>filename</i> archive]
<b>Release Information</b>	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 the maximum amount of data that the Junos OS logging utility writes to a log file <b>logfile</b> before archiving it (closing it, compressing it, and changing its name to <b>logfile.0.gz</b> ). The utility then opens and writes to a new file called <b>logfile</b> . For information about the number of archive files that the utility creates in this way, see <a href="#">files</a> .
<b>Options</b>	<p><b>size</b>—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</p> <p><b>Syntax:</b> <b>xk</b> to specify the number of kilobytes, <b>xm</b> for the number of megabytes, or <b>xg</b> for the number of gigabytes</p> <p><b>Range:</b> 64 KB through 1 GB</p> <p><b>Default:</b> 1 MB for MX Series routers and the QFX Series</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">files on page 1762</a></li> </ul>

## structured-data

---

<b>Syntax</b>	structured-data { brief; }
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system syslog file <i>filename</i> ], [edit system syslog file <i>filename</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. 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>	Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, <i>The syslog Protocol</i> ( <a href="http://tools.ietf.org/html/draft-ietf-syslog-protocol-23">http://tools.ietf.org/html/draft-ietf-syslog-protocol-23</a> ).
<div>  <p><b>NOTE:</b> When this statement is included, other statements that specify the format for messages written to the file are ignored (the <code>explicit-priority</code> statement at the [edit system syslog file <i>filename</i>] hierarchy level and the <code>time-format</code> statement at the [edit system syslog] hierarchy level).</p> </div>	
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Logging Messages in Structured-Data Format on page 1724</a></li> <li>• <i>Junos OS System Log Reference</i></li> <li>• <a href="#">explicit-priority on page 1759</a></li> <li>• <a href="#">time-format on page 1775</a></li> </ul>

## syslog (System)

```
Syntax syslog {
 allow-duplicates
 archive {
 (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);
 }
 console {
 facility severity;
 }
 file filename {
 facility severity;
 explicit-priority;
 match "regular-expression";
 archive {
 (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);
 }
 structured-data {
 brief;
 }
 }
 host (hostname | other-routing-engine | scc-master) {
 facility severity;
 explicit-priority;
 facility-override facility;
 log-prefix string;
 match "regular-expression";
 source-address source-address;
 structured-data {
 brief;
 }
 port port number;
 }
 log-rotate-frequency frequency;
 source-address source-address;
 time-format (millisecond | year | year millisecond);
 user (username | *) {
 facility severity;
 match "regular-expression";
 }
 }
```

**Hierarchy Level** [edit logical-systems *logical-system-name* system],  
[edit system]

<b>Release Information</b>	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. Support at the <b>[edit logical-systems <i>logical-system-name</i> system]</b> hierarchy level introduced in Junos OS Release 11.4.
<b>Description</b>	Configure the types of system log messages to log to files, a remote destination, user terminals, or the system console.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Junos OS System Log Overview on page 1717</a></li><li>• <a href="#">System Log Explorer</a></li></ul>


---

## system

---

<b>Syntax</b>	system { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure system management properties.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>System Management Configuration Statements</i></li></ul>

## time-format

<b>Syntax</b>	<code>time-format (year   millisecond   year millisecond);</code>
<b>Hierarchy Level</b>	<code>[edit system syslog]</code>
<b>Release Information</b>	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>	<p>Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a <b>file</b>, <b>console</b>, or <b>user</b> statement at the <code>[edit system syslog]</code> hierarchy level. As of Junos OS Release 11.4, the additional time information is also sent to destinations configured by a <b>host</b> statement.</p> <p>By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, <b>Aug 21 12:36:30</b>. However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the <code>[edit system syslog time-format]</code> statement.</p>
	<p> <b>NOTE:</b> When the <b>structured-data</b> statement is included at the <code>[edit system syslog file <i>filename</i>]</code> hierarchy level, this statement is ignored for the file.</p>
<b>Options</b>	<p><b>millisecond</b>—Include the millisecond in the timestamp.</p> <p><b>year</b>—Include the year in the timestamp.</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Including the Year or Millisecond in Timestamps on page 1727</a></li> <li>• <a href="#">System Log Explorer</a></li> <li>• <a href="#">structured-data on page 1772</a></li> </ul>

## traceoptions (Security Log)

<b>Syntax</b>	<pre> traceoptions {   file {     filename;     files number;     match regular-expression;     size maximum-file-size;     (world-readable   no-world-readable);   }   flag flag;   no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit security log]
<b>Release Information</b>	Statement modified in Release 9.2 of Junos OS.
<b>Description</b>	Configure security log tracing options.
<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 <b>/var/log</b>. 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 <b>size</b> 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 <b>trace-file</b> 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 <b>files</b> option and a filename.</p> <p>Syntax: <b>x K</b> to specify KB, <b>x m</b> to specify MB, or <b>x g</b> 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**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **configuration**—Trace configuration events
  - **hpl**— Trace HPL logging
  - **report**— Trace HPL logging
  - **source**—Communicate with security log forwarder
- **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.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">syslog (System) on page 1773</a></li></ul>
------------------------------	------------------------------------------------------------------------------------------------

## tracing

---

Syntax	<pre>tracing {   destination-override syslog host <i>ip-address</i>; }</pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	<p>Configure the router to enable remote tracing to a specified host IP address. The default setting is disabled.</p> <p>The following processes are supported:</p> <ul style="list-style-type: none"><li>• <b>chassisd</b>—Chassis-control process</li><li>• <b>eventd</b>—Event-processing process</li><li>• <b>cosd</b>—Class-of-service process</li><li>• <b>spd</b>—Adaptive-services process</li></ul> <p>You can use the <b>no-remote-trace</b> statement, under the [edit system process-name <b>traceoptions</b>] hierarchy, to disable remote tracing.</p>
Options	<b>destination-override syslog host <i>ip-address</i></b> —Overrides the global config under <b>system tracing</b> and has no effect if <b>system tracing</b> is not configured.
Required Privilege Level	<b>system</b> —To view this statement in the configuration. <b>system-control</b> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">destination-override on page 1757</a></li><li>• <a href="#">no-remote-trace (System) on page 1767</a></li></ul>



## user (System Logging)

<b>Syntax</b>	<pre> user (username   *) {     facility severity;     match "regular-expression"; } </pre>
<b>Hierarchy Level</b>	[edit system syslog]
<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>	Configure the logging of system messages to user terminals.
<b>Options</b>	<p><b>*</b> (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.</p> <p><b>facility</b>—Class of messages to log. To specify multiple classes, include multiple <b>facility severity</b> statements. For a list of the facilities, see <a href="#">Table 244 on page 1718</a>.</p> <p><b>severity</b>—Severity of the messages that belong to the facility specified by the paired <b>facility</b> name. Messages with severities the specified level and higher are logged. For a list of the severities, see <a href="#">Table 245 on page 1719</a>.</p> <p><b>username</b>—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one <b>user</b> statement.</p> <p>The remaining statement is explained separately.</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>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Directing System Log Messages to a User Terminal on page 1724</a></li> <li>• <a href="#">Junos OS System Logging Facilities and Message Severity Levels on page 1718</a></li> <li>• <a href="#">Junos OS System Log Reference</a></li> </ul>

## world-readable

---

<b>Syntax</b>	world-readable   no-world-readable;
<b>Hierarchy Level</b>	[edit system <a href="#">syslog archive</a> ], [edit system <a href="#">syslog file filename</a> archive]
<b>Release Information</b>	Statement introduced before OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Grant all users permission to read log files, or restrict the permission only to the <b>root</b> user and users who have the Junos <b>maintenance</b> permission.
<b>Default</b>	no-world-readable
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Specifying Log File Size, Number, and Archiving Properties</i></li><li>• <i>Junos OS System Log Reference</i></li></ul>

## Operational Commands

- [clear log](#)
- [clear security log](#)
- [clear security log file](#)
- [monitor list](#)
- [monitor start](#)
- [monitor stop](#)
- [show log](#)
- [show security log](#)
- [show security log file](#)

## clear log

<b>Syntax</b>	<code>clear log <i>filename</i></code> <code>&lt;all&gt;</code>
<b>Release Information</b>	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.
<b>Description</b>	Remove contents of a log file.
<b>Options</b>	<i>filename</i> —Name of the specific log file to delete.  <code>all</code> —(Optional) Delete the specified log file and all archived versions of it.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show log on page 1789</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear log on page 1781</a>

## Sample Output

### clear log

The following sample commands list log file information, clear the contents of a log file, and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:

-rw-r----- 1 root wheel 26450 Jun 23 18:47 /var/log/sampled
total 1

user@host> clear log lcc0-re0:sampled
lcc0-re0:

user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:

-rw-r----- 1 root wheel 57 Sep 15 03:44 /var/log/sampled
total 1
```

## clear security log

---

**Syntax** clear security log  
          <all>  
          <destination-address>  
          <destination-port>  
          <event-id>  
          <failure>  
          <interface-name>  
          <newer-than>  
          <older--than>  
          <process>  
          <protocol>  
          <severity>  
          <source-address>  
          <source-port>  
          <success>  
          <username>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Deletes the event log.

**Options** **all**—Clears all audit event logs stored in the device memory.

**destination-address**—Clears audit event logs with the specified destination address.

**destination-port**—Clears audit event logs with the specified destination port.

**event-id**—Clears audit event logs with the specified event identification number.

**failure**—Clears failed audit event logs.

**interface-name**—Clears audit event logs with the specified interface.

**newer-than**—Clears audit event logs newer than the specified date and time.

**older-than**—Clears audit event logs older than the specified date and time.

**process**—Clears audit event logs with the specified process that generated the event.

**protocol**—Clears audit event logs generated through the specified protocol.

**severity**—Clears audit event logs generated with the specified severity.

**source-address**—Clears audit event logs with the specified source address.

**source-port**—Clears audit event logs with the specified source port.

**success**—Clears successful audit event logs.

**username**—Clears audit event logs generated for the specified user.

**Required Privilege Level**    clear

**Related Documentation**

- [exclude \(Security Log\) on page 1758](#)
- [show security log on page 1791](#)

## Sample Output

clear security log all

```
user@host> clear security log all
7905 security log events cleared
```

## clear security log file

---

<b>Syntax</b>	clear security log file
<b>Release Information</b>	Command introduced in Release 12.1 of Junos OS.
<b>Description</b>	Deletes the content of an event mode security log file stored on the device in binary format.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security log file on page 1794</a></li></ul>

## Sample Output

### clear security log file

```
user@host> clear security log file
7905 security log events cleared
```

## monitor list

<b>Syntax</b>	monitor list
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display the status of monitored log and trace files.
<b>Options</b>	This command has no options.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">monitor start on page 1608</a></li> <li>• <a href="#">monitor stop on page 1610</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor list on page 1785</a>
<b>Output Fields</b>	<a href="#">Table 225 on page 1607</a> describes the output fields for the <b>monitor list</b> command. Output fields are listed in the approximate order in which they appear.

**Table 255: monitor list Output Fields**

Field Name	Field Description
<b>monitor start</b>	Indicates the file is being monitored.
<b>"filename"</b>	Name of the file that is being monitored.
<b>Last changed</b>	Date and time at which the file was last modified.

## Sample Output

### monitor list

```
user@host> monitor list
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)
```

## monitor start

<b>Syntax</b>	<code>monitor start <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Start displaying the system log or trace file and additional entries being added to those files.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols protocol]</b> hierarchy levels.



**NOTE:** To monitor a log file within a logical system, issue the `monitor start logical-system-name/filename` command.

<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">monitor list on page 1607</a></li> <li><a href="#">monitor stop on page 1610</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor start on page 1787</a>
<b>Output Fields</b>	<a href="#">Table 226 on page 1608</a> describes the output fields for the <b>monitor start</b> command. Output fields are listed in the approximate order in which they appear.

**Table 256: monitor start Output Fields**

Field Name	Field Description
<b>***<i>filename</i>***</b>	Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.
<b><i>Date and time</i></b>	Timestamp for the log entry.



## Sample Output

### monitor start

```
user@host> monitor start system-log
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: RSA key generation complete.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: RSA authentication for root accepted.
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from host.example.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
```

## monitor stop

---

<b>Syntax</b>	<code>monitor stop <i>filename</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Stop displaying the system log or trace file.
<b>Options</b>	<i>filename</i> —Specific log or trace file.
<b>Additional Information</b>	Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the <b>syslog</b> statement at the <b>[edit system]</b> hierarchy level and the <b>options</b> statement at the <b>[edit routing-options]</b> hierarchy level. The trace files generated by the routing protocol process are those configured with <b>traceoptions</b> statements at the <b>[edit routing-options]</b> , <b>[edit interfaces]</b> , and <b>[edit protocols <i>protocol</i>]</b> hierarchy levels.
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">monitor list on page 1607</a></li><li>• <a href="#">monitor start on page 1608</a></li></ul>
<b>List of Sample Output</b>	<a href="#">monitor stop on page 1788</a>
<b>Output Fields</b>	This command produces no output.

## Sample Output

### monitor stop

```
user@host> monitor stop
```

## show log

<b>List of Syntax</b>	<a href="#">Syntax on page 1789</a> <a href="#">Syntax (TX Matrix Router) on page 1789</a>
<b>Syntax</b>	<pre>show log &lt;filename   user &lt;username&gt;&gt;</pre>
<b>Syntax (TX Matrix Router)</b>	<pre>show log &lt;all-lcc   lcc number   scc&gt; &lt;filename   user &lt;username&gt;&gt;</pre>
<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>
<b>Description</b>	List log files, display log file contents, or display information about users who have logged in to the router or switch.
<b>Options</b>	<p><b>none</b>—List all log files.</p> <p><b>&lt;all-lcc   lcc number   scc&gt;</b>—(Routing matrix only) (Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace <i>number</i> with a value from <b>0</b> through <b>3</b>) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).</p> <p><b>filename</b>—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.</p> <p><b>user &lt;username&gt;</b>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include <i>username</i>, display logging information about the specified user.</p>
<b>Required Privilege Level</b>	trace
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">syslog (System) on page 1773</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show log on page 1789</a> <a href="#">show log filename on page 1790</a> <a href="#">show log user on page 1790</a>

## Sample Output

### show log

```
user@host> show log
total 57518
-rw-r--r-- 1 root bin 211663 Oct 1 19:44 dcd
-rw-r--r-- 1 root bin 999947 Oct 1 19:41 dcd.0
-rw-r--r-- 1 root bin 999994 Oct 1 17:48 dcd.1
-rw-r--r-- 1 root bin 238815 Oct 1 19:44 rpd
```

```

-rw-r--r-- 1 root bin 1049098 Oct 1 18:00 rpd.0
-rw-r--r-- 1 root bin 1061095 Oct 1 12:13 rpd.1
-rw-r--r-- 1 root bin 1052026 Oct 1 06:08 rpd.2
-rw-r--r-- 1 root bin 1056309 Sep 30 18:21 rpd.3
-rw-r--r-- 1 root bin 1056371 Sep 30 14:36 rpd.4
-rw-r--r-- 1 root bin 1056301 Sep 30 10:50 rpd.5
-rw-r--r-- 1 root bin 1056350 Sep 30 07:04 rpd.6
-rw-r--r-- 1 root bin 1048876 Sep 30 03:21 rpd.7
-rw-rw-r-- 1 root bin 19656 Oct 1 19:37 wtmp

```

### show log filename

```

user@host> show log rpd
Oct 1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct 1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct 1 18:00:18
Oct 1 18:00:19 KRT recv len 56 V9 seq 148 op add Type route/if af 2 addr
13.13.13.21 nhop type local nhop 13.13.13.21
Oct 1 18:00:19 KRT recv len 56 V9 seq 149 op add Type route/if af 2 addr
13.13.13.22 nhop type unicast nhop 13.13.13.22
Oct 1 18:00:19 KRT recv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct 1 18:00:19 KRT recv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct 1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct 1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct 1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...

```

### show log user

```

user@host> show log user
darius mg2546 Thu Oct 1 19:37 still logged in
darius mg2529 Thu Oct 1 19:08 - 19:36 (00:28)
darius mg2518 Thu Oct 1 18:53 - 18:58 (00:04)
root mg1575 Wed Sep 30 18:39 - 18:41 (00:02)
root ttyp2 jun.site.per Wed Sep 30 18:39 - 18:41 (00:02)
alex ttyp1 192.168.1.2 Wed Sep 30 01:03 - 01:22 (00:19)

```

## show security log

<b>Syntax</b>	<code>show security log {<i>all</i> <i>destination-address</i> <i>destination-port</i> <i>event-id</i> <i>failure</i> <i>interface-name</i> <i>newer-than</i> <i>older-than</i> <i>process</i> <i>protocol</i> <i>severity</i> <i>sort-by</i> <i>source-address</i> <i>source-port</i> <i>success</i> <i>user</i>}</code>
<b>Release Information</b>	Command introduced in Junos OS Release 11.2 .
<b>Description</b>	Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.
<b>Options</b>	<p><b>all</b>—Displays all audit event logs stored in the device memory.</p> <p><b>destination-address</b>—Displays audit event logs with the specified destination address.</p> <p><b>destination-port</b>—Displays audit event logs with the specified destination port.</p> <p><b>event-id</b>—Displays audit event logs with the specified event identification number.</p> <p><b>failure</b>—Displays failed audit event logs.</p> <p><b>interface-name</b>—Displays audit event logs with the specified interface.</p> <p><b>newer-than</b>—Displays audit event logs newer than the specified date and time.</p> <p><b>older-than</b>—Displays audit event logs older than the specified date and time.</p> <p><b>process</b>—Displays audit event logs with the specified process that generated the event.</p> <p><b>protocol</b>—Displays audit event logs generated through the specified protocol.</p> <p><b>severity</b>—Displays audit event logs generated with the specified severity.</p> <p><b>sort-by</b>—Displays audit event logs generated sorted with the specified options.</p> <p><b>source-address</b>—Displays audit event logs with the specified source address.</p> <p><b>source-port</b>—Displays audit event logs with the specified source port.</p> <p><b>success</b>—Displays successful audit event logs.</p> <p><b>username</b>—Displays audit event logs generated for the specified user.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">exclude (Security Log) on page 1758</a></li> <li>• <a href="#">clear security log on page 1782</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security log on page 1792</a>

**Output Fields** Table 257 on page 1792 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

**Table 257: show security log Output Fields**

Field Name	Field Description
Event time	The timestamp of the events received.  On SRX Series devices, security logs were always timestamped using the UTC time zone by running <b>set system time-zone utc</b> and <b>set security log utc-timestamp</b> CLI commands. Now, time zone can be defined using the local time zone by running the <b>set system time-zone time-zone</b> command to specify the local time zone that the system should use when timestamping the security logs.
Message	Security events are listed.

## Sample Output

### show security log

```

user@host> show security log
Event time Message
2010-10-22 13:28:37 CST session created 1.1.1.2/1->2.2.2.2/1308 icmp
1.1.1.2/1->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 52 N/A(N/A)
ge-0/0/1.0
2010-10-22 13:28:38 CST session created 1.1.1.2/2->2.2.2.2/1308 icmp
1.1.1.2/2->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0
...
2010-10-22 13:36:12 CST session denied 1.1.1.2/1->2.2.2.2/54812 icmp 1(8) policy1
trustZone untrustZone N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST session denied 1.1.1.2/2->2.2.2.2/54812 icmp 1(8) policy1
trustZone untrustZone N/A(N/A) ge-0/0/1.0
...
2010-10-27 15:50:11 CST IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
...
2011-02-18 15:53:34 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/cr1/ca-profile1.cr1
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv
...

```

```

2011-03-14 23:00:40 PDT IDP_COMMIT_COMPLETED: IDP policy commit is complete.
 IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;policy[
/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT]
 IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;policy[
/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT]
 IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;policy[
/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

, failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT]

...

Event time Message
2011-03-21 14:21:49 CST UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:05 CST KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:05 CST KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
tunnel, Type: dynamic
2011-03-21 14:23:08 CST UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST UI_CMDLINE_READ_LINE: User 'root', command 'show security
log '

```

## show security log file

<b>Syntax</b>	show security log file
<b>Release Information</b>	Command introduced in Release 12.1 of Junos OS.
<b>Description</b>	Enables customers to view event-mode log files stored on the device in binary format.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show security log on page 1791</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security log file on page 1794</a>
<b>Output Fields</b>	<a href="#">Table 258 on page 1794</a> lists the output fields for the <b>show security log file</b> command. Output fields are listed in the approximate order in which they appear.

**Table 258: show security log file Output Fields**

Field Name	Field Description
Event time	The timestamp when the security event was received.
Message	The message describing the security event.

## Sample Output

### show security log file

```

user@host> show security log file
<14>1 2011-08-28T21:14:43 topstar RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.34 source-address="7.7.7.2" source-port="1"
destination-address="8.8.8.2" destination-port="5636" service-name="icmp"
nat-source-address="7.7.7.2" nat-source-port="1" nat-destination-address="8.8.8.2"
nat-destination-port="5636" src-nat-rule-name="None" dst-nat-rule-name="None"
protocol-id="1" policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000442" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/0.0"]

<14>1 2011-08-28T21:14:45 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="7.7.7.2"
source-port="0" destination-address="8.8.8.2" destination-port="5636"
service-name="icmp" nat-source-address="7.7.7.2" nat-source-port="0"
nat-destination-address="8.8.8.2" nat-destination-port="5636"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="1"
policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000441" packets-from-client="1"
bytes-from-client="84" packets-from-server="1" bytes-from-server="84"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/0.0"]

...

user@host> show security log file

```



```
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]
```

```
<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]
```

```
<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]
```

```
...
```



## CHAPTER 36

# SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices

- [Overview on page 1797](#)
- [Network Monitoring Using SNMP on page 1799](#)
- [Remote Monitoring \(RMON\) with SNMP on page 1983](#)
- [Health Monitoring with SNMP on page 1998](#)
- [Configuration Statements and Operational Commands on page 2001](#)

## Overview

---

- [Introduction to Device Management on page 1797](#)

## Introduction to Device Management

- [Understanding Device Management Functions in Junos OS on page 1797](#)
- [Understanding the Integrated Local Management Interface on page 1799](#)

### 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 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 259 on page 1798](#).

Table 259: 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"> <li>Operational mode commands—For more information about operational mode commands, see the <i>CLI User Guide</i>.</li> <li>SNMP MIBs—For more information about SNMP MIBs supported by Junos OS, see “<a href="#">Standard SNMP MIBs Supported by Junos OS</a>” on page 1804 and “<a href="#">Juniper Networks Enterprise-Specific MIBs</a>” on page 1819.</li> <li>Standard SNMP traps—For more information about standard SNMP traps, see the “<a href="#">Standard SNMP Traps Supported on Devices Running Junos OS</a>” on page 1883.</li> <li>Enterprise-specific SNMP traps—For more information about enterprise-specific traps, see “<a href="#">Juniper Networks Enterprise-Specific SNMP Traps</a>” on page 1868.</li> <li>System log messages—For more information about how to configure system log messages, see <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i>.</li> </ul>
Configuration management	<ul style="list-style-type: none"> <li>Configure device attributes using the command-line interface (CLI). For more information about configuring the device using the CLI, see the <i>CLI User Guide</i>.</li> <li>Configuration Management MIB—For more information about the Configuration Management MIB, see the <i>Configuration Management MIB</i>.</li> </ul>
Accounting management	<p>Perform the following accounting-related tasks:</p> <ul style="list-style-type: none"> <li>Collect statistics for interfaces, firewall filters, destination classes, source classes, and the Routing Engine. For more information about collecting statistics, see “<a href="#">Accounting Options Configuration</a>” on page 1289.</li> <li>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.</li> <li>Count packets as part of a firewall filter. For more information about firewall filter policies, see “<a href="#">Juniper Networks Enterprise-Specific MIBs</a>” on page 1819 and the <i>Junos OS Routing Protocols Library for Security Devices</i>.</li> </ul>
Performance management	<p>Monitor performance in the following ways:</p> <ul style="list-style-type: none"> <li>Use operational mode commands. For more information about monitoring performance using operational mode commands, see the <i>CLI User Guide</i>.</li> <li>Use firewall filters. For more information about performance monitoring using firewall filters, see the <i>Junos OS Routing Protocols Library for Security Devices</i>.</li> </ul>

Table 259: 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"> <li>Control access to the router and authenticate users. For more information about access control and user authentication, see the <i>Junos OS User Authentication Library for Security Devices</i>.</li> <li>Control access to the router using SNMPv3 and SNMP over IPv6. For more information, see “Configuring the Local Engine ID” on page 1934 and “Tracing SNMP Activity on a Device Running Junos OS” on page 1969.</li> </ul>

- Related Documentation**
- [Understanding the SNMP Implementation in Junos OS on page 1800](#)
  - [Accounting Options Overview on page 1287](#)

### 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 on page 1797](#)

## Network Monitoring Using SNMP

- [SNMP MIBs Overview on page 1800](#)
- [SNMP MIBs and Traps Supported by Junos OS on page 1803](#)
- [Loading MIB Files to a Network Management System on page 1895](#)
- [Configuring SNMP on page 1897](#)
- [Configuring SNMPv3 on page 1916](#)
- [Configuring Routing Instances on page 1953](#)
- [Configuring Remote Operations on page 1959](#)
- [Tracing SNMP Activity on page 1969](#)

- [Configuring Vital MIB Data on page 1973](#)
- [SNMP FAQs on page 1981](#)

## SNMP MIBs Overview

- [Understanding the SNMP Implementation in Junos OS on page 1800](#)

### [Understanding the SNMP Implementation in Junos OS](#)

---

SNMP enables the monitoring of network devices from a central location. This topic provides an overview of SNMP and describes how SNMP is implemented in the Junos OS.

This topic includes the following sections:

- [SNMP Architecture on page 1800](#)
- [Junos OS SNMP Agent Features on page 1802](#)

#### ***SNMP Architecture***

The SNMP agent exchanges network management information with SNMP manager software running on a network management system (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.

This topic contains the following sections:

- [SNMP MIBs on page 1800](#)
- [SNMP Traps and Informs on page 1801](#)

#### ***SNMP MIBs***

A MIB is a hierarchy of information used to define managed objects in a network device. 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.

MIBs are either standard or enterprise-specific. Standard MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Depending on the vendor, many standard MIBs are delivered with the NMS software. You can also download the standard MIBs from the IETF website, [www.ietf.org](http://www.ietf.org), and compile them into your NMS, if necessary.

For a list of standard supported MIBs, see “[Standard SNMP MIBs Supported by Junos OS](#)” on page 1804.

Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific MIBs, you must obtain them from the manufacturer and compile them into your network management software.

For a list of Juniper Networks enterprise-specific supported MIBs, see “[Juniper Networks Enterprise-Specific MIBs](#)” on page 1819.

### ***SNMP Traps and Informs***

Routers can send notifications to SNMP managers when significant events occur on a network device, most often errors or failures. SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The standard traps are compiled into the network management software. You can also download the standard traps from the IETF website, [www.ietf.org](http://www.ietf.org).

For more information about standard traps supported by the Junos OS, see “[Standard SNMP Traps Supported on Devices Running Junos OS](#)” on page 1883.

Enterprise-specific traps are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific traps, you must obtain them from the manufacturer and compile them into your network management software.

For more information about enterprise-specific traps supported by the Junos OS, see “[Juniper Networks Enterprise-Specific SNMP Traps](#)” on page 1868. For information about system logging severity levels for SNMP traps, see “[System Logging Severity Levels for SNMP Traps](#)” on page 1802.

With traps, the receiver does not send any acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. An SNMP manager that receives an inform acknowledges the message with a response. For information about SNMP informs, see “[Configuring SNMP Informs](#)” on page 1935.

### ***SNMP Trap Queuing***

The 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.

The 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. The 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.

The 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 a 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, the throttle queue and the destination queue combined) is 40,000 traps. However, on EX Series switches, the maximum size of the trap queue is 1000 traps. The maximum size of any one queue is 20,000 traps for devices other than EX Series switches. On EX Series switches, the maximum size of one queue is 500 traps. If a trap is sent from a destination queue when the throttle queue has exceeded the maximum size, the trap is added back to the 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.



**NOTE:** Users cannot configure the Junos OS for trap queuing. Users cannot view any information about trap queues except what is available in the syslog.

---

### ***System Logging Severity Levels for SNMP Traps***

For some traps, when a trap condition occurs, regardless of whether the SNMP agent sends a trap to an NMS, the trap is logged if the system logging is configured to log an event with that system logging severity level. For more information about system logging severity levels, see the *System Log Monitoring and Troubleshooting Guide for Security Devices*.

For more information about system logging severity levels for standard traps, see [“Standard SNMP Version 1 Traps” on page 1884](#) and [“Standard SNMP Version 2 Traps” on page 1887](#). For more information about system logging severity levels for enterprise-specific traps, see [“Juniper Networks Enterprise-Specific SNMP Version 1 Traps” on page 1869](#) and [“Juniper Networks Enterprise-Specific SNMP Version 2 Traps” on page 1876](#).

### ***Junos OS SNMP Agent Features***

The Junos OS SNMP agent software consists of an SNMP master agent that delegates all SNMP requests to subagents. Each subagent is responsible for the support of a specific set of MIBs.

The Junos OS supports the following versions of SNMP:



- **SNMPv1**—The initial implementation of SNMP that defines the architecture and framework for SNMP.
- **SNMPv2c**—The revised protocol, with improvements to performance and manager-to-manager communications. Specifically, SNMPv2c implements community strings, which act as passwords when determining who, what, and how the SNMP clients can access the data in the SNMP agent. The community string is contained in SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests. The agent may require a different community string for **Get**, **GetBulk**, and **GetNext** requests (**read-only** access) than it does for **Set** requests (**read-write** access).
- **SNMPv3**—The most up-to-date protocol focuses on security. SNMPv3 defines a security model, user-based security model (USM), and a view-based access control model (VACM). SNMPv3 USM provides data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload. SNMPv3 VACM provides access control to determine whether a specific type of access (read or write) to the management information is allowed.

In addition, the Junos OS SNMP agent software accepts IPv4 and IPv6 addresses for transport over IPv4 and IPv6. For IPv6, the Junos OS supports the following features:

- SNMP data over IPv6 networks
- IPv6-specific MIB data
- SNMP agents for IPv6

**Related Documentation**

- *System Log Monitoring and Troubleshooting Guide for Security Devices*
- [SNMPv3 Overview on page 1916](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

## SNMP MIBs and Traps Supported by Junos OS

- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [List of SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways Supported Enterprise-Specific MIBs on page 1826](#)
- [List of SRX1400, SRX3400, and SRX3600 Services Gateways Supported Enterprise-Specific MIBs on page 1830](#)
- [List of SRX5400, SRX5600 and SRX5800 Services Gateways Supported Enterprise-Specific MIBs on page 1836](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1842](#)
- [MIB Support Details on page 1851](#)
- [SNMP MIB Objects Supported by Junos OS for the Set Operation on page 1861](#)
- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Juniper Networks Enterprise-Specific SNMP Version 1 Traps on page 1869](#)

- [Juniper Networks Enterprise-Specific SNMP Version 2 Traps on page 1876](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
- [Standard SNMP Version 1 Traps on page 1884](#)
- [Standard SNMP Version 2 Traps on page 1887](#)
- [Unsupported Standard SNMP Traps on page 1892](#)

### Standard SNMP MIBs Supported by Junos OS

Table 260 on page 1804 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 (M, T, MX, EX, 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 260: Standard MIBs Supported on Devices Running Junos OS**

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
IEEE 802.1ab section 12.1, <i>Link Layer Discovery Protocol (LLDP) MIB</i>	0	0	0	0	1	0	0	0
EX Series implementation of LLDP MIB supports both IPv4 and IPv6 configuration.								
IEEE, 802.3ad, <i>Aggregation of Multiple Link Segments</i>	0	1	1	1	1	1	1	1
Supported tables and objects:								
<ul style="list-style-type: none"> <li>• dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable</li> </ul>								
NOTE: EX Series switches do not support the dot3adAggPortTable and dot3adAggPortStatsTable.								
<ul style="list-style-type: none"> <li>• dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount)</li> </ul>								
NOTE: EX Series switches do not support the dot3adAggPortDebugTable.								
<ul style="list-style-type: none"> <li>• dot3adTablesLastChanged</li> </ul>								

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 1155, <i>Structure and Identification of Management Information for TCP/IP-based Internets</i>	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
RFC 1195, <i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i> (only the objects <b>isisSystem</b> , <b>isisMANAreaAddr</b> , <b>isisAreaAddr</b> , <b>isisSysProtSupp</b> , <b>isisSummAddr</b> , <b>isisCirc</b> , <b>isisCircLevel</b> , <b>isisPacketCount</b> , <b>isisSAdj</b> , <b>isisSAdjAreaAddr</b> , <b>isisAdjIPAddr</b> , <b>isisSAdjProtSupp</b> , <b>isisRa</b> , and <b>isisIPRA</b> are supported)	1	1	1	1	1	1	1	1
RFC 1212, <i>Concise MIB Definitions</i>	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	0	0	1
<ul style="list-style-type: none"> <li>• MIB II and its SNMP version 2 derivatives, including: <ul style="list-style-type: none"> <li>• Statistics counters</li> <li>• IP, except for <b>ipRouteTable</b>, which has been replaced by <b>ipCidrRouteTable</b> (RFC 2096, <i>IP Forwarding Table MIB</i>)</li> <li>• SNMP management</li> <li>• Interface management</li> </ul> </li> <li>• SNMPv1 <b>Get</b>, <b>GetNext</b> requests, and version 2 <b>GetBulk</b> request</li> <li>• Junos OS-specific secured access list</li> <li>• Master configuration keywords</li> <li>• Reconfigurations upon SIGHUP</li> </ul>								
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	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	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

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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 <b>pppLcp</b> 1 object and the tables <b>pppLinkStatustable</b> and <b>pppLinkConfigTable</b> ).	0	1	0	1	0	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
RFC 1695, <i>Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2</i>	1	1	1	0	0	0	0	0
RFC 1850, <i>OSPF Version 2 Management Information Base</i> (except for the <b>ospfOriginateNewLsas</b> and <b>ospfRxNewLsas</b> objects, the Host Table, and the traps <b>ospfOriginateLSA</b> , <b>ospfLsdbOverflow</b> , and <b>ospfLsdbApproachingOverflow</b> )	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
RFC 2011, <i>SNMPv2 Management Information Base for the Internet Protocol Using SMIv2</i>	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	0	1
RFC 2013, <i>SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2</i>	1	1	1	1	1	1	0	1
RFC 2024, <i>Definitions of Managed Objects for Data Link Switching Using SMIv2</i> (except for the <b>dlsWInterface</b> and <b>dlsWSDlc</b> object groups; the <b>dlsWDirLocateMacTable</b> , <b>dlsWDirNBTable</b> , and <b>dlsWDirLocateNBTable</b> tables; the <b>dlsWCircuitDiscReasonLocal</b> and <b>dlsWCircuitDiscReasonRemote</b> tabular objects; and the <b>dlsWDirMacCacheNextIndex</b> and <b>dlsWDirNBCacheNextIndex</b> scalar objects; read-only access)	0	1	1	1	0	0	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 2096, <i>IP Forwarding Table MIB</i> (The <b>ipCidrRouteTable</b> has been extended to include the tunnel name when the next hop is through an RSVP-signaled LSP.)  <b>NOTE:</b> RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.	1	1	1	1	1	0	0	1
RFC 2115, <i>Management Information Base for Frame Relay DTEs Using SMIv2</i> ( <b>frDlcmiTable</b> only; <b>frCircuitTable</b> and <b>frErrTable</b> are not supported)	0	1	1	1	0	1	0	0
RFC 2233, <i>The Interfaces Group MIB Using SMIv2</i>  <b>NOTE:</b> 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	0	1
RFC 2287, <i>Definitions of System-Level Managed Objects for Applications</i> (only the objects <b>sysApplInstallIPkgTable</b> , <b>sysApplInstallElmtTable</b> , <b>sysApplElmtRunTable</b> , and <b>sysApplMapTable</b> )	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	0	0
RFC 2495, <i>Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types</i> (except for <b>dsx1FarEndConfigTable</b> , <b>dsx1FarEndCurrentTable</b> , <b>dsx1FarEndIntervalTable</b> , <b>dsx1FarEndTotalTable</b> , and <b>dsx1FracTable</b> )	1	1	1	0	0	1	0	0
RFC 2515, <i>Definitions of Managed Objects for ATM Management</i> (except <b>atmVpCrossConnectTable</b> , <b>atmVcCrossConnectTable</b> , and <b>aal5VccTable</b> )	1	1	1	0	0	0	0	0
RFC 2570, <i>Introduction to Version 3 of the Internet-standard Network Management Framework</i>	1	1	1	1	1	0	0	1
RFC 2571, <i>An Architecture for Describing SNMP Management Frameworks</i> (read-only access)  <b>NOTE:</b> RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.	1	1	1	1	1	1	0	1

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 2572, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i> (read-only access)	1	1	1	1	1	1	0	1
<p><b>NOTE:</b> RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.</p>								
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	0	1
<p><b>NOTE:</b> RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.</p>								
RFC 2578, <i>Structure of Management Information Version 2 (SMIv2)</i>	1	1	1	1	1	0	0	1
RFC 2579, <i>Textual Conventions for SMIv2</i>	1	1	1	1	1	0	0	1
RFC 2580, <i>Conformance Statements for SMIv2</i>	1	1	1	1	1	0	0	1
RFC 2662, <i>Definitions of Managed Objects for ADSL Lines</i> (All MIB tables, objects, and traps are applicable for the ADSL ATU-R agent.)	0	1	1	1	0	1	0	0
RFC 2665, <i>Definitions of Managed Objects for the Ethernet-like Interface Types</i>	1	1	1	1	1	1	0	1
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i> (except row creation, the <b>Set</b> operation, and the object <b>vrpStatsPacketLengthErrors</b> )	1	1	1	1	1	1	0	1
RFC 2790, <i>Host Resources MIB</i>	1	1	1	1	1	1	0	1
<ul style="list-style-type: none"> <li>Only the <b>hrStorageTable</b>. The file systems <b>/</b>, <b>/config</b>, <b>/var</b>, and <b>/tmp</b> always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.</li> <li>Only the objects of the <b>hrSystem</b> and <b>hrSWInstalled</b> groups.</li> </ul>								

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 2819, <i>Remote Network Monitoring Management Information Base</i>	1	1	1	1	1	1	0	1
<ul style="list-style-type: none"> <li><b>etherStatsTable</b> (for Ethernet interfaces only), <b>alarmTable</b>, <b>eventTable</b>, and <b>logTable</b> are supported on all devices running Junos OS.</li> <li><b>historyControlTable</b> and <b>etherHistoryTable</b> (except <b>etherHistoryUtilization</b> object) are supported only on EX Series switches.</li> </ul>								
RFC 2863, <i>The Interfaces Group MIB</i>	1	1	1	1	1	0	0	1
<b>NOTE:</b> 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	0	0	1
RFC 2922, <i>The Physical Topology (PTOPO) MIB</i>	0	0	0	0	1	1	0	1
Supported objects:  <b>ptopoConnDiscAlgorithm,</b> <b>ptopoConnAgentNetAddrType,</b> <b>ptopoConnAgentNetAddr,</b> <b>ptopoConnMultiMacSASeen,</b> <b>ptopoConnMultiNetSASeen,</b> <b>ptopoConnsStatic,</b> <b>ptopoConnLastVerifyTime,</b> <b>ptopoConnRowStatus</b>								
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i> (only the objects <b>pingCtlTable</b> , <b>pingResultsTable</b> , <b>pingProbeHistoryTable</b> , <b>pingMaxConcurrentRequests</b> , <b>traceRouteCtlTable</b> , <b>traceRouteResultsTable</b> , <b>traceRouteProbeHistoryTable</b> , and <b>traceRouteHopsTable</b> )	1	1	1	1	1	1	0	1
RFC 2932, <i>IPv4 Multicast Routing MIB</i>	1	1	1	1	1	1	0	1
RFC 2934, <i>Protocol Independent Multicast MIB for IPv4</i>	1	1	1	1	1	1	0	0
<b>NOTE:</b> In Junos OS, RFC 2934 is implemented based on a draft version, <i>pimmib.mib</i> , of the now standard RFC.								
Support for the <b>pimNeighborLoss</b> trap was added in Release 11.4.								
RFC 2981, <i>Event MIB</i>	1	1	1	1	0	0	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 3014, <i>Notification Log MIB</i>	1	1	1	1	0	0	0	0
RFC 3019, <i>IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol</i>	0	1	1	1	0	0	0	1
RFC 3410 <i>Introduction and Applicability Statements for Internet-Standard Management Framework</i>	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	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	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	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	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	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	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	0	1
RFC 3418, <i>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</i>	1	1	1	1	1	0	0	1
NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.								



Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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 [ <b>jnxExperiment</b> ])	0	1	1	0	0	0	0	0
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	0	0	1
RFC 3591 <i>Managed Objects for the Optical Interface Type</i>  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)	0	1	1	0	0	0	0	0
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
RFC 3621, <i>Power Ethernet MIB</i>	0	0	0	0	1	0	0	0
RFC 3637, <i>Definitions of Managed Objects for the Ethernet WAN Interface Sublayer</i> (except etherWisDeviceTable, etherWisSectionCurrentTable, and etherWisFarEndPathCurrentTable)	0	1	1	1	0	0	0	0
RFC 3811, <i>Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management</i>	1	1	1	1	0	1	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	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	0	0	0
<ul style="list-style-type: none"> <li>MPLS tunnels as interfaces are not supported.</li> <li>The following objects in the <b>TunnelResource</b> table are not supported: <b>mplsTunnelResourceMeanRate</b>, <b>mplsTunnelResourceMaxBurstSize</b>, <b>mplsTunnelResourceMeanBurstSize</b>, <b>mplsTunnelResourceExBurstSize</b>, <b>mplsTunnelResourceWeight</b>.</li> <li><b>mplsTunnelPerfTable</b> and <b>mplsTunnelCRLDResTable</b> are not supported.</li> <li><b>mplsTunnelCHopTable</b> is supported on ingress routers only.</li> </ul> <p><b>NOTE:</b> The branch used by the proprietary LDP MIB (<b>ldpmib.mib</b>) conflicts with RFC 3812. <b>ldpmib.mib</b> has been deprecated and replaced by <b>jnx-mpls-ldp.mib</b>.</p>								
RFC 3813, <i>Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)</i> (read-only access). <b>mplsInterfacePerfTable</b> , <b>mplsInSegmentPerfTable</b> , <b>mplsOutSegmentPerfTable</b> , <b>mplsInSegmentMapTable</b> , <b>mplsXCUp</b> , and <b>mplsXCDown</b> are not supported.	1	1	1	1	0	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	0	0	1
RFC 3896, <i>Definitions of Managed Objects for the DS3/E3 Interface Type</i> (except <b>dsx3FarEndConfigTable</b> , <b>dsx3FarEndCurrentTable</b> , <b>dsx3FarEndIntervalTable</b> , <b>dsx3FarEndTotalTable</b> , and <b>dsx3FracTable</b> )	0	1	1	0	0	0	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	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"> <li>• <b>tunnelIfTable</b>—Provides information about the tunnels known to a router.</li> <li>• <b>tunnelInetConfigTable</b>—Assists dynamic creation of tunnels and provides mapping from end-point addresses to the current interface index value.</li> </ul> <b>NOTE:</b> Junos OS supports <b>MAX-ACCESS</b> of read-only for all the MIB objects in <b>tunnelIfTable</b> and <b>tunnelInetConfigTable</b> tables.	0	1	1	1	0	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"> <li>• <b>dot1dStp</b> subtree is supported on MX Series 3D Universal Edge Routers.</li> <li>• <b>dot1dTpFdbAddress</b>, <b>dot1dTpFdbPort</b>, and <b>dot1dTpFdbStatus</b> objects from the <b>dot1dTpFdbTable</b> of the <b>dot1dTp</b> subtree are supported on EX Series Ethernet Switches.</li> </ul> <b>NOTE:</b> <b>dot1dTpLearnedEntryDiscards</b> and <b>dot1dTpAgingTime</b> objects are supported on M and T Series routers.	0	0	0	1	1	0	0	0
RFC 4273, <i>Definitions of Managed Objects for BGP-4</i> (only <b>jnxBgpM2PrefixInPrefixes</b> , <b>jnxBgpM2PrefixInPrefixesAccepted</b> , and <b>jnxBgpM2PrefixInPrefixesRejected</b> objects)	1	1	1	1	1	0	0	1

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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"> <li>• <b>inetCidrRouteTable</b>—Provides the ability to display IP version-independent multipath CIDR routes and obsoletes the <b>ipCidrRouteTable</b> object.</li> <li>• <b>inetCidrRouteNumber</b>—Indicates the number of current routes and obsoletes the <b>ipCidrRouteNumber</b> object.</li> <li>• <b>inetCidrRouteDiscards</b>—Counts the number of valid routes that are discarded from <b>inetCidrRouteTable</b> and obsoletes the <b>ipCidrRouteDiscards</b> object.</li> </ul> <p><b>NOTE:</b> Junos OS currently supports these MIB objects that will be deprecated in future releases: <b>ipCidrRouteTable</b>, <b>ipCidrRouteNumber</b>, and <b>ipCidrRouteDiscards</b>.</p>	1	1	1	1	1	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
RFC 4363b, <i>Q-Bridge VLAN MIB</i>	0	0	0	1	1	0	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	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	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"> <li>• <code>mplsL3VpnActiveVrfs</code></li> <li>• <code>mplsL3VpnConfiguredVrfs</code></li> <li>• <code>mplsL3VpnConnectedInterfaces</code></li> <li>• <code>mplsL3VpnVrfConfMidRteThresh</code></li> <li>• <code>mplsL3VpnVrfConfHighRteThresh</code></li> <li>• <code>mplsL3VpnIfConfRowStatus</code></li> <li>• <code>mplsL3VpnIILblRcvThrsh</code></li> <li>• <code>mplsL3VpnNotificationEnable</code></li> <li>• <code>mplsL3VpnVrfConfMaxPossRts</code></li> <li>• <code>mplsL3VpnVrfConfRteMxThrshTime</code></li> <li>• <code>mplsL3VpnVrfOperStatus</code></li> <li>• <code>mplsL3VpnVrfPerfCurrNumRoutes</code></li> <li>• <code>mplsL3VpnVrfPerfTable</code></li> <li>• <code>mplsL3VpnVrfRteTable</code></li> <li>• <code>mplsVpnVrfRTTable</code></li> <li>• <code>mplsL3VpnVrfSecIllegalLblVltns</code></li> <li>• <code>mplsL3VpnVrfTable</code></li> </ul> <p><b>NOTE:</b> 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	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
RFC 4670, <i>RADIUS Accounting Client Management Information Base (MIB)</i> (read-only access)	0	0	0	1	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

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	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). <b>gmplsTunnelReversePerfTable</b> , <b>gmplsTeScalars</b> , <b>gmplsTunnelTable</b> , <b>gmplsTunnelARHopTable</b> , <b>gmplsTunnelCHopTable</b> , and <b>gmplsTunnelErrorTable</b> are not supported.)	0	1	1	1	0	0	0	0
RFC 4803, <i>Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base (MIB)</i> (read-only access). <b>gmplsLabelTable</b> and <b>gmplsOutsegmentTable</b> are not supported.	0	1	1	1	0	0	0	0
<b>NOTE:</b> 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 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 5643, <i>Management Information Base for OSPFv3</i>	0	1	1	1	0	0	0	1
<p><b>NOTE:</b> 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"> <li>• ospfv3HostTable</li> <li>• ospfv3CfgNbrTable</li> <li>• ospfv3ExitOverflowInterval</li> <li>• ospfv3ReferenceBandwidth</li> <li>• ospfv3RestartSupport</li> <li>• ospfv3RestartInterval</li> <li>• ospfv3RestartStrictLsaChecking</li> <li>• ospfv3RestartStatus</li> <li>• ospfv3RestartAge</li> <li>• ospfv3RestartExitReason</li> <li>• ospfv3NotificationEnable</li> <li>• ospfv3StubRouterSupport</li> <li>• ospfv3StubRouterAdvertisement</li> <li>• ospfv3DiscontinuityTime</li> <li>• ospfv3RestartTime</li> <li>• ospfv3AreaNssaTranslatorRole</li> <li>• ospfv3AreaNssaTranslatorState</li> <li>• ospfv3AreaNssaTranslatorStabInterval</li> <li>• ospfv3AreaNssaTranslatorEvents</li> <li>• ospfv3AreaTEEnabled</li> <li>• ospfv3IfMetricValue</li> <li>• ospfv3IfDemandNbrProbe</li> </ul>								
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
Internet Assigned Numbers Authority, <i>IANAiftype Textual Convention MIB</i> (referenced by RFC 2233, available at <a href="http://www.iana.org/assignments/ianaiftype-mib">http://www.iana.org/assignments/ianaiftype-mib</a> )	1	1	1	1	1	1	0	0

Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	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
Internet draft draft-ietf-bfd-mib-02.txt, <i>Bidirectional Forwarding Detection Management Information Base</i> (Represented by <b>mib-jnx-bfd-exp.txt</b> and implemented under the Juniper Networks enterprise branch [jnxExperiment]. Read only. Includes <b>bfdSessUp</b> and <b>bfdSessDown</b> traps. Does not support <b>bfdSessPerfTable</b> and <b>bfdSessMapTable</b> .)	1	1	1	1	1	0	0	1
Internet draft draft-ietf-idmr-igmp-mib-13.txt, <i>Internet Group Management Protocol (IGMP) MIB</i>	0	1	1	1	1	0	0	1
Internet draft draft-reeder-snmpp3-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	0	0	1
Internet draft draft-ietf-isis-wg-mib-07.txt, <i>Management Information Base for IS-IS</i> (only <b>isisSAdjTable</b> , <b>isisSAdjAreaAddrTable</b> , <b>isisSAdjIPAddrTable</b> , and <b>isisSAdjProtSuppTable</b> )  <b>NOTE:</b> Replaced with RFC 4444, <i>IS-IS MIB</i> in Junos OS Release 11.3 and later.	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 <b>mplsVpnScalars</b> , <b>mplsVpnVrfTable</b> , <b>mplsVpnPerTable</b> , and <b>mplsVpnVrfRouteTargetTable</b> )	0	1	1	1	0	0	0	0
Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, <i>Management Information Base for OSPFv3</i> (Represented by <b>mib-jnx-ospfv3mib.txt</b> and implemented under the Juniper Networks enterprise branch [jnxExperiment]. Support for <b>ospfv3NbrTable</b> only. Read only. Object names are prefixed by <b>jnx</b> . For example, <b>jnxOspfv3NbrTable</b> , <b>jnxOspfv3NbrAddressType</b> , and <b>jnxOspfv3NbrPriority</b> .)	0	1	1	1	0	0	0	1
Internet draft draft-ietf-idmr-pim-mib-09.txt, <i>Protocol Independent Multicast (PIM) MIB</i>	1	1	1	1	1	0	0	1



Table 260: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	ACX	M	T	MX	EX	SRX		
						Low-End	Mid-Range	High-End
ESO Consortium MIB, which can be found at <a href="http://www.snmp.com/eso/">http://www.snmp.com/eso/</a>	1	1	1	1	1	1	0	0
<b>NOTE:</b> The ESO Consortium MIB has been replaced by RFC 3826.								
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	0	0	0

**Related Documentation**

- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Loading MIB Files to a Network Management System on page 1895](#)

### Juniper Networks Enterprise-Specific MIBs

The 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/junos12.3x48/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt).

For more information, see *Alarm 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/junos12.3x48/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-atm.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-chas-defines.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chas-defines.txt).

For more information, see *Chassis MIBs*.

- Chassis Forwarding MIB—This MIB extends the scope of health monitoring to include Junos forwarding process (**fwdd**) components. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-fwdd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-fwdd.txt).

For more information, see *Chassis Forwarding MIB*.

- 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/junos12.3x48/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt).

For more information, see *Destination Class Usage 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt).

For more information, see *DNS Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt).

For more information, see *Event 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/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt).

For more information, see *Firewall 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/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 all SRX Series devices. 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-idp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt).

For more information, see *Interface MIB*.

- IP Forward MIB—Extends the standard IP Forwarding Table MIB (RFC 2096) to include CIDR forwarding information. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt).

For more information, see *IP Forward 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-ipv6.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipv6.txt).

For more information, see *IPv6 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/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt).

For more information about logical systems MIBs and downloadable versions of the MIBs, see *Logical Systems 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt).

For more information, see *NAT Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt).

For more information, see *Packet Forwarding Engine 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/junos12.3x48/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt).

For more information, see *Policy Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt).

For more information, see *RMON Events and Alarms 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt).

For more information, see *Security Screening Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-scu.txt).

For more information, see *Source Class Usage MIB*.

- SPU Monitoring MIB—Provides support for monitoring SPUs on all high-end SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt).

For more information, see *SPU Monitoring Objects MIB*.

- Structure of Management Information MIB—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.

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/junos12.3x48/topics/reference/mibs/mib-jnx-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-smi.txt).

For more information, see *Structure of Management Information 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/junos12.3x48/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt).

For more information, see *Traceroute MIB*.

- Utility MIB—Provides SNMP support for exposing 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/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt).

For more information, see *Utility MIB*.

- 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-vpn.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-vpn.txt).

For more information, see *VPN MIB*.

**Related  
Documentation**

- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1842](#)
- [Loading MIB Files to a Network Management System on page 1895](#)

---

### List of SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways Supported Enterprise-Specific MIBs

---

Junos OS supports the following enterprise-specific MIBs:

- Structure of Management Information MIB—Contains object identifiers (OIDs) for the security branch of the MIBs used in Junos OS for SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for SRX Series devices. It also 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-smi.txt). For more information, see *Structure of Management Information 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt).

For more information, see *Alarm 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/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt).

For more information, see *BGP4 V2 MIB*.



- **BFD 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/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt).

For more information, see *Bidirectional Forwarding Detection MIB*.

- **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 Switching Board (SSB), Switching and Forwarding Model (SFM), Flexible PIC Concentrators (FPCs), and PICs. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis.txt).

For more information, see *Chassis MIBs*.

- **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/junos12.3x48/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-cfgmgmt.txt).

For more information, see *Configuration Management 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/junos12.3x48/topics/reference/mibs/mib-jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt).

For more information, see *Event 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/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt).

For more information, see *Firewall MIB*.

- **Host Resources MIB**—Extends the **hrStorageTable** object, providing a measure of the usage of each file system on the router in percentage. 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/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt).

For more information, see *Host Resources 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/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt).

For more information, see *Interface MIB*.

- IP Forward MIB—Extends the standard IP Forwarding Table MIB (RFC 2096) to include CIDR forwarding information. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt).

For more information, see *IP Forward 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt).

For more information, see *IPsec Monitoring 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt).

For more information, see *IPsec Generic Flow Monitoring Object 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt).

For more information, see *IPv4 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/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt).

For more information, see *License MIB*.

- Network Address Translation (NAT) Objects MIB—Provides support for monitoring network address translation (NAT). This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/](http://www.juniper.net/techpubs/en_US/junos12.3x48/)

[topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt) .

For more information, see *NAT Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt) .

For more information, see *Packet Forwarding Engine 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/junos12.3x48/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt) .

For more information, see *Policy Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 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/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt) .

For more information, see *RMON Events and Alarms MIB*.

- Security Interface Extension Objects MIB—Provides support for the security management of interfaces. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-if-ext.txt) .

For more information, see *Security Interface Extension Objects MIB*.

- **SNMP 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-idp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-idp.txt).

For more information, see *SNMP IDP 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/junos12.3x48/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-syslog.txt).

For more information, see *System Log MIB*.

- **Traceroute MIB**—Supports the Junos 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/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt).

For more information, see *Traceroute MIB*.

- **Utility MIB**—Provides SNMP support for exposing Junos data and has tables that contain information on each type of data, such as integer and string. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt).

For more information, see *Utility MIB*.

- **VPN Certificate Objects MIB**—Provides support for monitoring the local and CA certificates loaded on the router. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt).

For more information, see *VPN Certificate Objects MIB*.

**Related  
Documentation**

- *System Log Monitoring and Troubleshooting Guide for Security Devices*
- *Structure of Management Information MIB*

---

### List of SRX1400, SRX3400, and SRX3600 Services Gateways Supported Enterprise-Specific MIBs

---

Junos OS supports the following enterprise-specific MIBs:

- Structure of Management Information MIB—Contains object identifiers (OIDs) for the security branch of the MIBs used in Junos OS for SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for SRX Series devices. It also 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/junos12.1x46/topics/reference/mibs/mib-jnx-js-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-smi.txt). For more information, see *Structure of Management Information MIB*.

- 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt).

For more information, see *Alarm MIB*.

- ATM CoS 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/junos12.3x48/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-atm-cos.txt).

For more information, see *ATM Class-of-Service 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/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt).

For more information, see *BGP4 V2 MIB*.

- BFD 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/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt).

For more information, see *Bidirectional Forwarding Detection MIB*.

- 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 Switching Board (SSB), Switching and Forwarding Model (SFM), Flexible PIC Concentrators (FPCs), and PICs. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-jsrpd.txt).

For more information, see *Chassis Cluster 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/junos12.3x48/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 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/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt).

For more information, see *Destination Class Usage MIB*.

- DNS Objects MIB—Provides support for monitoring DNS proxy queries, requests, responses, and failures. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt).

For more information, see *DNS Objects MIB*.

- Ethernet MAC MIB—Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, **inocets**, **inframes**, **outocets**, 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/junos12.3x48/topics/reference/mibs/mib-jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt).

For more information, see *Event 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/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt).

For more information, see *Firewall MIB*.

- Host Resources MIB—Extends the **hrStorageTable** object, providing a measure of the usage of each file system on the router in percentage. 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/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt).

For more information, see *Host Resources 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/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt).

For more information, see *Interface MIB*.

- IP Forward MIB—Extends the standard IP Forwarding Table MIB (RFC 2096) to include CIDR forwarding information. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt).

For more information, see *IP Forward 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt).

For more information, see *IPsec Monitoring 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt).

For more information, see *IPsec Generic Flow Monitoring Object 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt).

For more information, see *IPv4 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/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt).

For more information, see *License MIB*.

- Logical Systems MIB—Provides support for logical systems security profile. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt).

For more information, see *Logical Systems 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt).

For more information, see *NAT Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt).

For more information, see *Packet Forwarding Engine 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/junos12.3x48/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt).

For more information, see *Policy Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt).

For more information, see *RMON Events and Alarms 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt).

For more information, see *Security Screening Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt).

For more information, see *SPU Monitoring Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt) .

For more information, see *Traceroute MIB*.

- Utility MIB—Provides SNMP support for exposing 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/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt) .

For more information, see *Utility MIB*.

- 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/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt) .

For more information, see *VPN Certificate Objects MIB*.

#### Related Documentation

- *Structure of Management Information MIB*

---

### List of SRX5400, SRX5600 and SRX5800 Services Gateways Supported Enterprise-Specific MIBs

---

Junos OS supports the following enterprise-specific MIBs:

- Structure of Management Information MIB—Contains object identifiers (OIDs) for the security branch of the MIBs used in Junos OS for SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for SRX Series devices. It also explains how the Juniper Networks enterprise-specific MIBs are structured. For a downloadable version of this MIB, [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-smi.txt) . For more information, see *Structure of Management Information MIB*.
- 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis-alarm.txt).

For more information, see *Alarm MIB*.

- ATM CoS 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/junos12.3x48/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-atm-cos.txt).

For more information, see *ATM Class-of-Service 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/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bgpmib2.txt).

For more information, see *BGP4 V2 MIB*.

- BFD 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/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-bfd.txt).

For more information, see *Bidirectional Forwarding Detection MIB*.

- 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 Switching Board (SSB), Switching and Forwarding Model (SFM), Flexible PIC Concentrators (FPCs), and PICs. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-jsrpd.txt).

For more information, see *Chassis Cluster 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/junos12.3x48/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 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/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-dcu.txt).

For more information, see *Destination Class Usage MIB*.

- DNS Objects MIB—Provides support for monitoring DNS proxy queries, requests, responses, and failures. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-dns.txt).

For more information, see *DNS Objects MIB*.

- Ethernet MAC MIB—Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, **inocets**, **inframes**, **outocets**, 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/junos12.3x48/topics/reference/mibs/jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/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/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-event.txt).

For more information, see *Event 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/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-firewall.txt).

For more information, see *Firewall MIB*.

- Host Resources MIB—Extends the **hrStorageTable** object, providing a measure of the usage of each file system on the router in percentage. 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/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-hostresources.txt).

For more information, see *Host Resources 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/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-if-extensions.txt).

For more information, see *Interface MIB*.

- **IP Forward MIB**—Extends the standard IP Forwarding Table MIB (RFC 2096) to include CIDR forwarding information. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipforward.txt).

For more information, see *IP Forward 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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt).

For more information, see *IPsec Monitoring 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/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-ipv4.txt).

For more information, see *IPv4 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/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-license.txt).

For more information, see *License MIB*.

- **Logical Systems MIB**—Provides support for logical systems security profile. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt).

For more information, see *Logical Systems MIB*.

- Network Address Translation (NAT) Objects MIB—Provides support for monitoring network address translation (NAT). This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-nat.txt) .

For more information, see *NAT Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-pfe.txt) .

For more information, see *Packet Forwarding Engine 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/junos12.3x48/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-policy.txt) .

For more information, see *Policy Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-rmon.txt) .

For more information, see *RMON Events and Alarms MIB*.

- Security Interface Extension Objects MIB—Provides support for the security management of interfaces. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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 only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-screening.txt).

For more information, see *Security Screening Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt).

For more information, see *SPU Monitoring Objects 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/junos12.3x48/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/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/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-traceroute.txt).

For more information, see *Traceroute MIB*.

- Utility MIB—Provides SNMP support for exposing Junos OS data and has tables that contain information on each type of data, such as integer and string. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-util.txt).

For more information, see *Utility MIB*.

- VPN Certificate Objects MIB—Provides support for monitoring the local and CA certificates loaded on the router. This MIB is currently supported only by Junos OS for SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.3x48/topics/reference/mibs/mib-jnx-js-cert.txt).

For more information, see *VPN Certificate Objects MIB*.

#### Related Documentation

- *Structure of Management Information MIB*

### Enterprise-Specific MIBs and Supported Devices

Table 261 on page 1842 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 (M, MX, T, EX, J, 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 (SRX100, SRX110, SRX210, SRX220, and SRX240), Mid-Range (SRX550 and SRX650), and High-End (SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800).

Table 261: Enterprise-Specific MIBs and Supported Devices

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
AAA Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-user-aaa.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-user-aaa.txt</a>	1	1	0	0	0	0	1	1
Access Authentication Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-auth.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-auth.txt</a>	0	0	0	0	1	1	1	1
Alarm MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis-alarm.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis-alarm.txt</a>	1	1	1	1	1	1	1	1



Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
Analyzer MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-analyzer.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-analyzer.txt</a>	0	0	0	1	0	0	0	0
Antivirus Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-utm-av.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-utm-av.txt</a>	0	0	0	0	0	1	0	0
ATM Class-of-Service MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-atm-cos.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-atm-cos.txt</a>	1	1	1	0	0	1	0	1
ATM MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-atm.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-atm.txt</a>	1	1	1	0	0	0	0	0
BGP4 V2 MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-bgpmib2.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-bgpmib2.txt</a>	1	1	1	1	1	1	1	1
Bidirectional Forwarding Detection MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-bfd.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-bfd.txt</a>	1	1	1	1	1	1	1	1
Chassis Forwarding MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis-fwdd.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis-fwdd.txt</a>	0	0	0	0	1	1	0	0
Chassis MIBs <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chassis.txt</a> <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chas-defines.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-chas-defines.txt</a>	1	1	1	1	1	1	1	1
Chassis Cluster MIBs <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jsrpd.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jsrpd.txt</a>	0	0	0	0	0	0	1	1

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
Class-of-Service MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-cos.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-cos.txt</a>	1	1	1	1	1	0	0	1
Configuration Management MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-cfgmgmt.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-cfgmgmt.txt</a>	1	1	1	1	1	1	1	1
Destination Class Usage MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dcu.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dcu.txt</a>	1	1	1	0	1	0	1	1
DHCP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jdhcp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jdhcp.txt</a>	1	1	1	0	0	0	0	0
DHCPv6 MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jdhcpv6.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jdhcpv6.txt</a>	1	1	1	0	0	0	0	0
Digital Optical Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dom.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dom.txt</a>	1	0	1	0	0	0	0	0
DNS Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-dns.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-dns.txt</a>	0	0	0	0	0	0	1	1
Dynamic Flow Capture MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dfc.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-dfc.txt</a>	1	1	1	0	0	0	0	0
Ethernet MAC MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/jnx-mac.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/jnx-mac.txt</a>	1	1	1	1	1	0	0	1

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
Event MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-event.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-event.txt</a>	1	1	1	1	1	1	1	1
EX Series MAC Notification MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ex-mac-notification.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ex-mac-notification.txt</a>	0	0	0	1	0	0	0	0
EX Series SMI MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ex-smi.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ex-smi.txt</a>	0	0	0	1	0	0	0	0
Experimental MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-exp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-exp.txt</a>	1	1	1	1	1	0	0	0
Firewall MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-firewall.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-firewall.txt</a>	1	1	1	1	1	1	1	1
Flow Collection Services MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-coll.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-coll.txt</a>	1	1	1	0	0	0	0	0
Host Resources MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-hostresources.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-hostresources.txt</a>	1	1	1	1	1	1	1	1
Interface MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-if-extensions.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-if-extensions.txt</a>	1	1	1	1	1	1	1	1
IP Forward MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipforward.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipforward.txt</a>	1	1	1	1	1	1	1	1

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
IPsec Generic Flow Monitoring Object MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt</a>	0	0	0	0	1	0	0	1
IPsec Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt</a>	1	1	1	0	1	0	0	1
IPsec VPN Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt</a>	0	0	0	0	1	1	0	0
IPv4 MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipv4.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipv4.txt</a>	1	1	1	1	1	1	1	1
IPv6 and ICMPv6 MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipv6.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ipv6.txt</a>	1	1	1	1	0	1	1	1
L2ALD MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2ald.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2ald.txt</a>	0	1	0	1	0	0	0	
L2CP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2cp-features.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2cp-features.txt</a>	0	0	0	1	0	0	0	
L2TP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2tp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-l2tp.txt</a>	1	1	0	0	0	0	0	0
LDP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ldp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ldp.txt</a>	1	1	1	0	0	0	0	1

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
License MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-license.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-license.txt</a>	1	1	1	0	0	1	1	1
Logical Systems MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt</a>	0	0	0	0	0	0	1	1
MIMSTP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mimstp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mimstp.txt</a>	0	1	0	1	0	0	0	0
MPLS LDP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mpls-ldp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mpls-ldp.txt</a>	1	1	1	0	1	0	0	0
MPLS MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mpls.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-mpls.txt</a>	1	1	1	1	1	0	0	1
NAT Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-nat.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-nat.txt</a>	0	0	0	0	1	1	1	1
NAT Resources-Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sp-nat.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sp-nat.txt</a>	1	1	1	0	0	0	0	0
OTN Interface Management MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-otn.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-otn.txt</a>	1	1	1	0	0	0	0	0
Packet Forwarding Engine MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pfe.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pfe.txt</a>	1	1	1	0	1	1	1	1

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
Packet Mirror MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-packet-mirror.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-packet-mirror.txt</a>	0	1	0	0	0	0	0	0
PAE Extension MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pae-extension.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pae-extension.txt</a>	0	0	0	1	0	0	0	0
Passive Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pmon.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pmon.txt</a>	1	1	1	0	0	0	0	0
Ping MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ping.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ping.txt</a>	1	1	1	1	1	1	1	1
Policy Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-policy.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-policy.txt</a>	0	0	0	0	1	1	1	1
Power Supply Unit MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-power-supply-unit.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-power-supply-unit.txt</a>	0	0	0	1	0	0	0	0
PPP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ppp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-ppp.txt</a>	1	1	0	0	0	0	0	0
PPPoE MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pppoe.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pppoe.txt</a>	1	1	0	0	0	0	0	0
Psuedowire TDM MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pwtdm.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-pwtdm.txt</a>	1	1	1	0	0	0	0	0

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
Real-Time Performance Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rpm.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rpm.txt</a>	1	1	1	1	1	1	0	0
Reverse-Path-Forwarding MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rpf.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rpf.txt</a>	1	1	1	0	1	1	1	1
RMON Events and Alarms MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rmon.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rmon.txt</a>	1	1	1	0	1	1	1	1
RSVP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rsvp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-rsvp.txt</a>	1	1	1	0	0	0	0	0
Security Interface Extension Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-if-ext.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-if-ext.txt</a>	0	0	0	0	1	1	1	1
Security Screening Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-screening.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-screening.txt</a>	0	0	0	0	0	0	0	1
Services PIC MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sp.txt</a>	1	1	1	0	0	0	0	0
SNMP IDP MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-idp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-idp.txt</a>	0	0	0	0	0	1	1	1
SONET APS MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sonetaps.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sonetaps.txt</a>	1	1	1	0	0	0	0	0

Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
SONET/SDH Interface Management MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sonet.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-sonet.txt</a>	1	1	1	0	0	0	0	0
Source Class Usage MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-scu.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-scu.txt</a>	1	1	1	0	0	0	0	1
SPU Monitoring MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt</a>	0	0	0	0	0	1	1	1
Structure of Management Information MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-smi.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-smi.txt</a>	1	1	1	1	1	1	1	1
Subscriber MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-subscriber.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-subscriber.txt</a>	0	1	0	0	0	0	0	0
System Log MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-syslog.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-syslog.txt</a>	1	1	1	1	1	1	1	1
Traceroute MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-traceroute.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-traceroute.txt</a>	1	1	1	1	1	1	1	1
Utility MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-util.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-util.txt</a>	1	1	1	1	1	1	1	1
Virtual Chassis MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-virtualchassis.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-virtualchassis.txt</a>	0	0	0	1	0	0	0	0



Table 261: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
VLAN MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vlan.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vlan.txt</a>	0	0	0	1	0	0	0	0
VPLS MIBs <ul style="list-style-type: none"> <li><a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-generic.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-generic.txt</a></li> <li><a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-ldp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-ldp.txt</a></li> <li><a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-bgp.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpls-bgp.txt</a></li> </ul>	1	1	1	1	0	0	0	0
VPN Certificate Objects MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-cert.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-js-cert.txt</a>	0	0	0	0	1	1	1	1
VPN MIB <a href="http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpn.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-vpn.txt</a>	1	1	1	0	1	0	0	0

**Related Documentation**

- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Loading MIB Files to a Network Management System on page 1895](#)

**MIB Support Details**

Table 262 on page 1851 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 262: MIB Support for Routing Instances (Juniper Networks MIBs)

Object	Support Class	Description/Notes
jnxProducts(1)	–	Product Object IDs
jnxServices(2)	–	Services

**Table 262: MIB Support for Routing Instances (Juniper Networks MIBs) (continued)**

Object	Support Class	Description/Notes
<b>jnxMibs(3)</b> <b>jnxBoxAnatomy(1)</b>	Class 3	Objects are exposed only for the default logical system.
<b>mpls(2)</b>	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
<b>ifJnx(3)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxAlarms(4)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxFirewalls(5)</b>	Class 4	Data is not segregated by routing instance. All instances are exposed.
<b>jnxDCUs(6)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxPingMIB(7)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxTraceRouteMIB(8)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxATM(10)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxIpv6(11)</b>	Class 4	Data is not segregated by routing instance. All instances are exposed.
<b>jnxIpv4(12)</b>	Class 1	<b>jnxIpv4AddrTable(1)</b> . Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxRmon(13)</b>	Class 3	<b>jnxRmonAlarmTable(1)</b> . Objects are exposed only for the default logical system.
<b>jnxLdp(14)</b>	Class 2	<b>jnxLdpTrapVars(1)</b> . All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.

Table 262: MIB Support for Routing Instances (Juniper Networks MIBs) (*continued*)

Object	Support Class	Description/Notes
<b>jnxCos(15)</b> <b>jnxCosIfqStatsTable(1)</b> <b>jnxCosFcTable(2)</b> <b>jnxCosFcIdTable(3)</b> <b>jnxCosQstatTable(4)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxScu(16)</b> <b>jnxScuStatsTable(1)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxRpf(17)</b> <b>jnxRpfStatsTable(1)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxCfgMgmt(18)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxPMon(19)</b> <b>jnxPMonFlowTable(1)</b> <b>jnxPMonErrorTable(2)</b> <b>jnxPMonMemoryTable(3)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxSonet(20)</b> <b>jnxSonetAlarmTable(1)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxAtmCos(21)</b> <b>jnxCosAtmVcTable(1)</b> <b>jnxCosAtmScTable(2)</b> <b>jnxCosAtmVcQstatsTable(3)</b> <b>jnxCosAtmTrunkTable(4)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>ipSecFlowMonitorMIB(22)</b>	—	—
<b>jnxMac(23)</b> <b>jnxMacStats(1)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>apsMIB(24)</b>	Class 3	Objects are exposed only for the default logical system.
<b>jnxChassisDefines(25)</b>	Class 3	Objects are exposed only for the default logical system.

**Table 262: MIB Support for Routing Instances (Juniper Networks MIBs) (continued)**

Object	Support Class	Description/Notes
<b>jnxVpnMIB(26)</b>	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
<b>jnxSericesInfoMib(27)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxCollectorMIB(28)</b>	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
<b>jnxHistory(29)</b>	—	—
<b>jnxSpMIB(32)</b>	Class 3	Objects are exposed only for the default logical system.

[Table 263 on page 1855](#) 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 263: 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 263: Class 1 MIB Objects (Standard and Juniper MIBs) (*continued*)

Class	MIB	Objects
	rfc3020.mib	<b>mfrMIB</b> <b>mfrBundleTable</b> <b>mfrMibBundleLinkObjects</b> <b>mfrBundleIfIndexMappingTable</b> (and related MIB objects)
	ospf2mib.mib	All objects
	ospf2trap.mib	All objects
	bgpmib.mib	All objects
	rfc2819a.mib	Example: <b>etherStatsTable</b>

Table 263: 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 263: 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 264 on page 1859 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 264: Class 2 MIB Objects (Standard and Juniper MIBs)

Class	MIB	Objects
Class 2	rfc3813.mib	<b>mplsLsrStdMIB</b>  Examples:  <b>mplsInterfaceTable</b>  <b>mplsInSegmentTable</b>  <b>mplsOutSegmentTable</b>  <b>mplsLabelStackTable</b>  <b>mplsXCTable</b>  (and related MIB objects)
	igmpmib.mib	<b>igmpStdMIB</b>
	l3vpn.mib	<b>mplsVpnMIB</b>
	jnx-mpls.mib	Example: <b>mplsLspList</b>
	jnx-ldp.mib	<b>jnxLdp</b>  Example: <b>jnxLdpStatsTable</b>
	jnx-vpn.mib	<b>jnxVpnMIB</b>
	jnx-bgp.mib	<b>jnxBgpM2Experiment</b>

[Table 265 on page 1860](#) 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 265: 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 266 on page 1861](#) 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 266: 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 1953](#)
- [Trap Support for Routing Instances on page 1954](#)

### SNMP MIB Objects Supported by Junos OS for the Set Operation

Table 267 on page 1861 lists the SNMP MIB objects that are supported by Junos OS for the **snmp set** operation.

Table 267: SNMP MIB Objects

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	1.3.6.1.2.1.11.30

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
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

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
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

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
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

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
jnxPingCtlEgressJitterThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.12
jnxPingCtlIngressTimeThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.13
jnxPingCtlIngressStdDevThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.14
jnxPingCtlIngressJitterThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.15
jnxPingTrapGeneration	1.3.6.1.4.1.2636.3.7.1.2.1.16
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

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
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



Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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
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

Table 267: SNMP MIB Objects (*continued*)

Object Name	Object Identifier
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	
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 1804](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1842](#)

### 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 on page 1869](#)
- [Juniper Networks Enterprise-Specific SNMP Version 2 Traps on page 1876](#)
- [Juniper Networks Enterprise-Specific BGP 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 Library for Routing Devices.

- [Juniper Networks Enterprise-Specific Traps on EX Series Switches](#)
- [Juniper Networks Enterprise-Specific Traps on MX Series 3D Universal Edge Routers](#)

- Related Documentation**
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
  - [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
  - [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
  - [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
  - [Managing Traps and Informs on page 1981](#)

### Juniper Networks Enterprise-Specific SNMP Version 1 Traps

The Junos OS supports enterprise-specific SNMP version 1 traps shown in [Table 268 on page 1869](#). The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

For more information about system log messages, see the [System Log Explorer](#). To view the Juniper Networks enterprise-specific SNMP version 2 traps, see “[Juniper Networks Enterprise-Specific SNMP Version 2 Traps](#)” on page 1876. For more information about chassis traps, see *Chassis Traps*.

**Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps**

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
<b>Chassis Notifications (Alarm Conditions)</b>							
<i>Chassis MIB</i> (jnx-chassis.mib)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1	6	1	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFanFailure	1.3.6.1.4.1.2636.4.1	6	2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1	6	3	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxRedundancySwitchOver	1.3.6.1.4.1.2636.4.1	6	4	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
	<b>jnxFruPowerOff</b>	1.3.6.1.4.1.2636.4.1	6	7	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruPowerOn</b>	1.3.6.1.4.1.2636.4.1	6	8	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruFailed</b>	1.3.6.1.4.1.2636.4.1	6	9	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruOffline</b>	1.3.6.1.4.1.2636.4.1	6	10	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruOnline</b>	1.3.6.1.4.1.2636.4.1	6	11	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruCheck</b>	1.3.6.1.4.1.2636.4.1	6	12	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFEBSwitchover</b>	1.3.6.1.4.1.2636.4.1	6	13	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxHardDiskFailed</b>	1.3.6.1.4.1.2636.4.1	6	14	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxHardDiskMissing</b>	1.3.6.1.4.1.2636.4.1	6	15	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxPowerSupplyOk</b>	1.3.6.1.4.1.2636.4.2	6	1	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFanOK</b>	1.3.6.1.4.1.2636.4.2	6	2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxTemperatureOK</b>	1.3.6.1.4.1.2636.4.2	6	3	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
<b>Configuration Notifications</b>							
<i>Configuration Management MIB (jnx-configmgmt.mib)</i>	<b>jnxCmCfgChange</b>	1.3.6.1.4.1.2636.4.5	6	1	–	–	All devices running Junos OS.
	<b>jnxCmRescueChange</b>	1.3.6.1.4.1.2636.4.5	6	2	–	–	All devices running Junos OS.

Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
<b>Link Notifications</b>							
<i>Flow Collection Services MIB (jnx-coll.mib)</i>	<b>jnxCollUnavailableDest</b>	1.3.6.1.4.1.2636.4.8	6	1	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollUnavailableDestCleared</b>	1.3.6.1.4.1.2636.4.8	6	2	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollUnsuccessfulTransfer</b>	1.3.6.1.4.1.2636.4.8	6	3	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFlowOverload</b>	1.3.6.1.4.1.2636.4.8	6	4	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFlowOverloadCleared</b>	1.3.6.1.4.1.2636.4.8	6	5	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollMemoryUnavailable</b>	1.3.6.1.4.1.2636.4.8	6	6	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollMemoryAvailable</b>	1.3.6.1.4.1.2636.4.8	6	7	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFtpSwitchover</b>	1.3.6.1.4.1.2636.4.8	6	8	–	–	Devices that run Junos OS and have collector PICs installed.

Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
<i>Passive Monitoring MIB</i> (jnx-pmonmib)	jnxPMonOverloadSet	1.3.6.1.4.1.2636.4.7.0.1	6	1	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
	jnxPMonOverloadCleared	1.3.6.1.4.1.2636.4.7.0.2	6	2	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
<i>SONET APS MIB</i> (jnx-sonetaps.mib)	apsEventChannelMismatch	1.3.6.1.4.1.2636.3.24.2	6	3	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventPSBF	1.3.6.1.4.1.2636.3.24.2	6	4	–	–	Devices that run Junos OS and have SONET PICs installed.
	apsEventFEPLF	1.3.6.1.4.1.2636.3.24.2	6	5	–	–	Devices that run Junos OS and have SONET PICs installed.
<b>Remote Operations</b>							
<i>PING MIB</i> (jnx-ping.mib)	jnxPingRttThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	1	–	–	All devices running Junos OS.
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	2	–	–	All devices running Junos OS.
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	3	–	–	All devices running Junos OS.
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	4	–	–	All devices running Junos OS.

Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
	<b>jnxPingEgressStdDevThresholdExceeded</b>	1.3.6.1.4.1.2636.4.9	6	5	–	–	All devices running Junos OS.
	<b>jnxPingEgressJitterThresholdExceeded</b>	1.3.6.1.4.1.2636.4.9	6	6	–	–	All devices running Junos OS.
	<b>jnxPingIngressThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9	6	7	–	–	All devices running Junos OS.
	<b>jnxPingIngressStddevThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9	6	8	–	–	All devices running Junos OS.
	<b>jnxPingIngressJitterThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9	6	9	–	–	All devices running Junos OS.
<b>Routing Notifications</b>							
<i>BFD Experimental MIB (jnx-bfd-exp.mib)</i>	<b>bfdSessUp</b>	1.3.6.1.4.1.2636.5.3.1	6	1	–	–	All devices running Junos OS.
	<b>bfdSessDown</b>	1.3.6.1.4.1.2636.5.3.1	6	2	–	–	All devices running Junos OS.
<i>LDP MIB (jnx-ldp.mib)</i>	<b>jnxLdpLspUp</b>	1.3.6.1.4.1.2636.4.4	6	1	–	–	M, T, and MX Series routers.
	<b>jnxLdpLspDown</b>	1.3.6.1.4.1.2636.4.4	6	2	–	–	M, T, and MX Series routers.
	<b>jnxLdpSesUp</b>	1.3.6.1.4.1.2636.4.4	6	3	–	–	M, T, and MX Series routers.
	<b>jnxLdpSesDown</b>	1.3.6.1.4.1.2636.4.4	6	4	–	–	M, T, and MX Series routers.



Table 268: Juniper Networks Enterprise-Specific Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag	Supported On
<i>MPLS MIB</i> ( <i>jnx-mpls.mib</i> )	<b>mplsLspUp</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	1	–	–	
	<b>mplsLspDown</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	2	–	–	
	<b>mplsLspChange</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	3	–	–	
	<b>mplsLspPathDown</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4	6	4	–	–	
<i>VPN MIB</i> ( <i>jnx-vpn.mib</i> )	<b>jnxVpnIfUp</b>	1.3.6.1.4.1.2636.3.2.6	6	1	–	–	M, T, and MX Series routers.
	<b>jnxVpnIfDown</b>	1.3.6.1.4.1.2636.3.2.6	6	2	–	–	M, T, and MX Series routers.
	<b>jnxVpnPwUp</b>	1.3.6.1.4.1.2636.3.2.6	6	3	–	–	M, T, and MX Series routers.
	<b>jnxVpnPwDown</b>	1.3.6.1.4.1.2636.3.2.6	6	4	–	–	M, T, and MX Series routers.
<b>RMON Alarms</b>							
<i>RMON MIB</i> ( <i>jnx-rmon.mib</i> )	<b>jnxRmonAlarmGetFailure</b>	1.3.6.1.4.1.2636.4.3	6	1	–	–	All devices running Junos OS.
	<b>jnxRmonGetOk</b>	1.3.6.1.4.1.2636.4.3	6	2	–	–	All devices running Junos OS.
<b>SONET Alarms</b>							
<i>SONET MIB</i> ( <i>jnx-sonet.mib</i> )	<b>jnxSonetAlarmSet</b>	1.3.6.1.4.1.2636.4.6	6	1	–	–	Devices that run Junos OS and have SONET PICs installed.
	<b>jnxSonetAlarmCleared</b>	1.3.6.1.4.1.2636.4.6	6	2	–	–	Devices that run Junos OS and have SONET PICs installed.

- Related Documentation**
- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
  - [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
  - [Juniper Networks Enterprise-Specific MIBs on page 1819](#)

- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Managing Traps and Informs on page 1981](#)

### Juniper Networks Enterprise-Specific SNMP Version 2 Traps

The Junos OS supports the enterprise-specific SNMP version 2 traps shown in [Table 269 on page 1876](#). The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

For more information about system messages, see the [System Log Explorer](#). For more information about configuring system logging, see the [Junos OS Administration Library for Routing Devices](#). To view the Juniper Networks enterprise-specific SNMP version 1 traps, see “[Juniper Networks Enterprise-Specific SNMP Version 1 Traps](#)” on page 1869. For more information about chassis traps, see *Chassis Traps*.

**Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps**

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<b>Chassis (Alarm Conditions) Notifications</b>					
<i>Chassis MIB (jnx-chassis.mib)</i>	<b>jnxPowerSupplyFailure</b>	1.3.6.1.4.1.2636.4.1.1	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFanFailure</b>	1.3.6.1.4.1.2636.4.1.2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxOverTemperature</b>	1.3.6.1.4.1.2636.4.1.3	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxRedundancySwitchOver</b>	1.3.6.1.4.1.2636.4.1.4	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruRemoval</b>	1.3.6.1.4.1.2636.4.1.5	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruInsertion</b>	1.3.6.1.4.1.2636.4.1.6	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruPowerOff</b>	1.3.6.1.4.1.2636.4.1.7	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruPowerOn</b>	1.3.6.1.4.1.2636.4.1.8	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
	<b>jnxFruFailed</b>	1.3.6.1.4.1.2636.4.1.9	Warning	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruOffline</b>	1.3.6.1.4.1.2636.4.1.10	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruOnline</b>	1.3.6.1.4.1.2636.4.1.11	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFruCheck</b>	1.3.6.1.4.1.2636.4.1.12	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFEBSwitchover</b>	1.3.6.1.4.1.2636.4.1.13	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxHardDiskFailed</b>	1.3.6.1.4.1.2636.4.1.14	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxHardDiskMissing</b>	1.3.6.1.4.1.2636.4.1.15	Notice	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxPowerSupplyOK</b>	1.3.6.1.4.1.2636.4.2.1	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxFanOK</b>	1.3.6.1.4.1.2636.4.2.2	Critical	CHASSISD_SNMP_TRAP	All devices running Junos OS.
	<b>jnxTemperatureOK</b>	1.3.6.1.4.1.2636.4.2.3	Alert	CHASSISD_SNMP_TRAP	All devices running Junos OS.
<b>Configuration Notifications</b>					
<i>Configuration Management MIB (jnx-cfgmgmt.mib)</i>	<b>jnxCmCfgChange</b>	1.3.6.1.4.1.2636.4.5.0.1	–	–	All devices running Junos OS.
	<b>jnxCmRescueChange</b>	1.3.6.1.4.1.2636.4.5.0.2	–	–	All devices running Junos OS.
<b>Link Notifications</b>					

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<i>Flow Collection Services MIB (jnx-coll.mib)</i>	<b>jnxCollUnavailableDest</b>	1.3.6.1.4.1.2636.4.8.0.1	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollUnavailableDestCleared</b>	1.3.6.1.4.1.2636.4.8.0.2	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollUnsuccessfulTransfer</b>	1.3.6.1.4.1.2636.4.8.0.3	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFlowOverload</b>	1.3.6.1.4.1.2636.4.8.0.4	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFlowOverloadCleared</b>	1.3.6.1.4.1.2636.4.8.0.5	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollMemoryUnavailable</b>	1.3.6.1.4.1.2636.4.8.0.6	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollMemoryAvailable</b>	1.3.6.1.4.1.2636.4.8.0.7	–	–	Devices that run Junos OS and have collector PICs installed.
	<b>jnxCollFtpSwitchover</b>	1.3.6.1.4.1.2636.4.8.0.8	–	–	Devices that run Junos OS and have collector PICs installed.
<i>PMON MIB (jnx-pmon.mib)</i>	<b>jnxPMonOverloadSet</b>	1.3.6.1.4.1.2636.4.7.0.1	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.
	<b>jnxPMonOverloadCleared</b>	1.3.6.1.4.1.2636.4.7.0.2	–	–	Devices that run Junos OS and have PICs that support passive monitoring installed.

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<i>SONET APS MIB (jnx-sonetaps.mib)</i>	<b>apsEventChannelMismatch</b>	1.3.6.1.4.1.2636.3.24.2.0.3	–	–	Devices that run Junos OS and have SONET PICs installed.
	<b>apsEventPSBF</b>	1.3.6.1.4.1.2636.3.24.2.0.4	–	–	Devices that run Junos OS and have SONET PICs installed.
	<b>apsEventFEPLF</b>	1.3.6.1.4.1.2636.3.24.2.0.5	–	–	Devices that run Junos OS and have SONET PICs installed.
<b>Remote Operations Notifications</b>					
<i>PING MIB (jnx-ping.mib)</i>	<b>jnxPingRttThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.1	–	–	All devices running Junos OS.
	<b>jnxPingRttStdDevThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.2	–	–	All devices running Junos OS.
	<b>jnxPingRttJitterThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.3	–	–	All devices running Junos OS.
	<b>jnxPingEgressThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.4	–	–	All devices running Junos OS.
	<b>jnxPingEgressStdDevThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.5	–	–	All devices running Junos OS.
	<b>jnxPingEgressJitterThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.6	–	–	All devices running Junos OS.
	<b>jnxPingIngressThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.7	–	–	All devices running Junos OS.
	<b>jnxPingIngressStddevThreshold Exceeded</b>	1.3.6.1.4.1.2636.4.9.0.8	–	–	All devices running Junos OS.
<i>BFD Experimental MIB (jnx-bfd-exp.mib)</i>	<b>bfdSessUp</b>	1.3.6.1.4.1.2636.5.3.1.0.1	–	–	All devices running Junos OS.
	<b>bfdSessDown</b>	1.3.6.1.4.1.2636.5.3.1.0.2	–	–	All devices running Junos OS.
<b>Routing Notifications</b>					
<i>BFD Experimental MIB (jnx-bfd-exp.mib)</i>	<b>bfdSessUp</b>	1.3.6.1.4.1.2636.5.3.1.0.1	–	–	All devices running Junos OS.
	<b>bfdSessDown</b>	1.3.6.1.4.1.2636.5.3.1.0.2	–	–	All devices running Junos OS.

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<i>BGP4 V2 MIB</i> (jnx-bgpmib2.mib)	jnxBgpM2Established	1.3.6.1.4.1.2636.5.1.1.1.0.1	–	–	All devices running Junos OS.
	jnxBgpM2BackwardTransition	1.3.6.1.4.1.2636.5.1.1.1.0.2	–	–	All devices running Junos OS.
<i>DHCP MIB</i> (jnx-dhcp.mib)	jnxJdhcpLocalServer DuplicateClient	1.3.6.1.4.1.2636.3.6.1.6.1.13.1	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer InterfaceLimitExceeded	1.3.6.1.4.1.2636.3.6.1.6.1.13.2	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer InterfaceLimitAbated	1.3.6.1.4.1.2636.3.6.1.6.1.13.3	–	–	All devices running Junos OS.
	jnxJdhcpLocalServer Health	1.3.6.1.4.1.2636.3.6.1.6.1.13.4	–	–	All devices running Junos OS.
	jnxJdhcpRelayInterface LimitExceeded	1.3.6.1.4.1.2636.3.6.1.6.1.23.1	–	–	All devices running Junos OS.
	jnxJdhcpRelayInterface LimitAbated	1.3.6.1.4.1.2636.3.6.1.6.1.23.2	–	–	All devices running Junos OS.
<i>DHCPv6 MIB</i> (jnx-dhcpv6.mib)	jnxJdhcpv6LocalServer InterfaceLimitExceeded	1.3.6.1.4.1.2636.3.6.2.6.2.23.1	–	–	All devices running Junos OS.
	jnxJdhcpv6LocalServer InterfaceLimitAbated	1.3.6.1.4.1.2636.3.6.2.6.2.23.2	–	–	All devices running Junos OS.
	jnxJdhcpv6LocalServer Health	1.3.6.1.4.1.2636.3.6.2.6.2.23.3	–	–	All devices running Junos OS.
<i>LDP MIB</i> (jnx-ldp.mib)	jnxLdpLspUp	1.3.6.1.4.1.2636.4.4.0.1	–	–	M, T, and MX Series routers.
	jnxLdpLspDown	1.3.6.1.4.1.2636.4.4.0.2	–	–	M, T, and MX Series routers.
	jnxLdpSesUp	1.3.6.1.4.1.2636.4.4.0.3	–	–	M, T, and MX Series routers.
	jnxLdpSesDown	1.3.6.1.4.1.2636.4.4.0.4	–	–	M, T, and MX Series routers.

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<i>MPLS MIB</i> (jnx-mpls.mib)	<b>mplsLspUp</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4.1	–	–	
	<b>mplsLspInfoUp</b>	1.3.6.1.4.1.2636.3.2.0.1	–	–	M, T, and MX Series routers.
	<b>mplsLspDown</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4.2	–	–	
	<b>mplsLspInfoDown</b>	1.3.6.1.4.1.2636.3.2.0.2	–	–	M, T, and MX Series routers.
	<b>mplsLspChange</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4.3	–	–	
	<b>mplsLspInfoChange</b>	1.3.6.1.4.1.2636.3.2.0.3	–	–	M, T, and MX Series routers.
	<b>mplsLspPathDown</b> (Deprecated)	1.3.6.1.4.1.2636.3.2.4.4	–	–	
	<b>mplsLspInfoPathDown</b>	1.3.6.1.4.1.2636.3.2.0.4	–	–	M, T, and MX Series routers.
	<b>mplsLspInfoPathUp</b>	1.3.6.1.4.1.2636.3.2.0.5	–	–	M, T, and MX Series routers.
<i>VPN MIB</i> (jnx-vpn.mib)	<b>jnxVpnIfUp</b>	1.3.6.1.4.1.2636.3.26.0.1	–	–	M, T, and MX Series routers.
	<b>jnxVpnIfDown</b>	1.3.6.1.4.1.2636.3.26.0.2	–	–	M, T, and MX Series routers.
	<b>jnxVpnPwUp</b>	1.3.6.1.4.1.2636.3.26.0.3	–	–	M, T, and MX Series routers.
	<b>jnxVpnPwDown</b>	1.3.6.1.4.1.2636.3.26.0.4	–	–	M, T, and MX Series routers.

Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
AAA MIB (jnx-user-aaa.mib)	jnxAccessAuthAddressPoolHighThreshold	1.3.6.1.4.1.2636.3.51.1.0.5	–	–	SRX Series devices.
	jnxAccessAuthAddressPoolAbateThreshold	1.3.6.1.4.1.2636.3.51.1.0.6	–	–	SRX Series devices.
	jnxAccessAuthAddressPoolOutOfAddresses	1.3.6.1.4.1.2636.3.51.1.0.7	–	–	SRX Series devices.
	jnxAccessAuthAddressPoolOutOfMemory	1.3.6.1.4.1.2636.3.51.1.0.8	–	–	SRX Series devices.
	jnxAccessAuthService Up	1.3.6.1.4.1.2636.3.51.1.0.1	–	–	SRX Series devices.
	jnxAccessAuthService Down	1.3.6.1.4.1.2636.3.51.1.0.2	–	–	SRX Series devices.
	jnxAccessAuthServer Disabled	1.3.6.1.4.1.2636.3.51.1.0.3	–	–	SRX Series devices.
	jnxAccessAuthServer Enabled	1.3.6.1.4.1.2636.3.51.1.0.4	–	–	SRX Series devices.
Access Authentication Methods MIB (jnx-js-auth.mib)	jnxJsFwAuthFailure	1.3.6.1.4.1.2636.3.39.1.2.1.0.1	–	–	SRX Series devices.
	jnxJsFwAuthServiceUp	1.3.6.1.4.1.2636.3.39.1.2.1.0.2	–	–	SRX Series devices.
	jnxJsFwAuthServiceDown	1.3.6.1.4.1.2636.3.39.1.2.1.0.3	–	–	SRX Series devices.
	jnxJsFwAuthCapacityExceeded	1.3.6.1.4.1.2636.3.39.1.2.1.0.4	–	–	SRX Series devices.
Network Address Translation Resources-Monitoring MIB (jnxNatMIB)	jnxJsNatAddrPoolThresholdStatus	1.3.6.1.4.1.2636.3.39.1.7.1.0.1	–	–	SRX Series devices.
	jnxNatAddrPoolUtil	1.3.6.1.4.1.2636.3.59.1.2.1	–	–	M Series and MX Series routers
	jnxNatTrapSrcPoolName	1.3.6.1.4.1.2636.3.59.1.2.2	–	–	M Series and MX Series routers
	jnxNatAddrPoolThresholdStatus	1.3.6.1.4.1.2636.3.59.1.0.1	–	–	M Series and MX Series routers



Table 269: Juniper Networks Enterprise-Specific Supported SNMP Version 2 Traps (*continued*)

Source MIB	Trap Name	snmpTrapOID	System Logging Severity Level	System Log Tag	Supported On
<i>Network Address Translation MIB</i> (jnx-js-nat.mib)	jnxJsScreen Attack	1.3.6.1.4.1.2636.3.39.1.8.1.0.1	Warning	RT_SCREEN_ICMP, RT_SCREEN_IP, RT_SCREEN_SESSION_LIMIT, RT_SCREEN_TCP, RT_SCREEN_UDP	SRX Series devices.
<i>Security Screening Objects MIB</i> (jnx-js-screening.mib)	jnxJsScreenCfg Change	1.3.6.1.4.1.2636.3.39.1.8.1.0.2	—	—	SRX Series devices.
<b>RMON Alarms</b>					
<i>RMON MIB</i> (jnx-rmon.mib)	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3.0.2	—	—	All devices running Junos OS.
<b>SONET Alarms</b>					
<i>SONET MIB</i> (jnx-sonet.mib)	jnxSonetAlarm Cleared	1.3.6.1.4.1.2636.4.6.0.2	—	—	Devices that run Junos OS and have SONET PICs installed.

**Related Documentation**

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Managing Traps and Informs on page 1981](#)

**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 on page 1884](#)
- [Standard SNMP Version 2 Traps on page 1887](#)

- [Unsupported Standard SNMP Traps on page 1892](#)

#### Related Documentation

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Managing Traps and Informs on page 1981](#)

### Standard SNMP Version 1 Traps

Table 270 on page 1884 provides an overview of the standard traps for SNMPv1. The traps are organized first by trap category and then by trap name, and include their enterprise ID, generic trap number, and specific trap number. The system logging severity levels are listed for those traps that have them with their corresponding system log tag. Traps that do not have corresponding system logging severity levels are marked with an en dash (–) in the table.

For more information about system log messages, see the [System Log Explorer](#). For more information about configuring system logging, see the *Junos OS System Basics Configuration Guide*.

**Table 270: Standard Supported SNMP Version 1 Traps**

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
<b>Startup Notifications</b>							
RFC 1215, <i>Conventions for Defining Traps for Use with the SNMP</i>	<b>authenticationFailure</b>	1.3.6.1.4.1.2636	4	0	Notice	SNMPD_TRAP_GEN_FAILURE	All devices running Junos OS.
	<b>coldStart</b>	1.3.6.1.4.1.2636	0	0	Critical	SNMPD_TRAP_COLD_START	All devices running Junos OS.
	<b>warmStart</b>	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_WARM_START	All devices running Junos OS.
<b>Link Notifications</b>							
RFC 1215, <i>Conventions for Defining Traps for Use with the SNMP</i>	<b>linkDown</b>	1.3.6.1.4.1.2636	2	0	Warning	SNMP_TRAP_LINK_DOWN	All devices running Junos OS.
	<b>linkUp</b>	1.3.6.1.4.1.2636	3	0	Info	SNMP_TRAP_LINK_UP	All devices running Junos OS.
<b>Remote Operations Notifications</b>							

Table 270: Standard Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i>	<b>pingProbeFailed</b>	1.3.6.1.2.1.80.0	6	1	Info	SNMP_TRAP_PING_PROBE_FAILED	All devices running Junos OS.
	<b>pingTestFailed</b>	1.3.6.1.2.1.80.0	6	2	Info	SNMP_TRAP_PING_TEST_FAILED	All devices running Junos OS.
	<b>pingTestCompleted</b>	1.3.6.1.2.1.80.0	6	3	Info	SNMP_TRAP_PING_TEST_COMPLETED	All devices running Junos OS.
	<b>traceRoutePathChange</b>	1.3.6.1.2.1.81.0	6	1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE	All devices running Junos OS.
	<b>traceRouteTestFailed</b>	1.3.6.1.2.1.81.0	6	2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED	All devices running Junos OS.
	<b>traceRouteTestCompleted</b>	1.3.6.1.2.1.81.0	6	3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED	All devices running Junos OS.
<b>RMON Alarms</b>							
RFC 2819a, <i>RMON MIB</i>	<b>fallingAlarm</b>	1.3.6.1.2.1.16	6	2	—	—	All devices running Junos OS.
	<b>risingAlarm</b>	1.3.6.1.2.1.16	6	1	—	—	All devices running Junos OS.
<b>Routing Notifications</b>							
<i>BGP 4 MIB</i>	<b>bgpEstablished</b>	1.3.6.1.2.1.15.7	6	1	—	—	M, T, MX, J, EX, and SRX for branch devices.
	<b>bgpBackwardTransition</b>	1.3.6.1.2.1.15.7	6	2	—	—	M, T, MX, J, EX, and SRX for branch devices.

Table 270: Standard Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
<i>OSPF TRAP MIB</i>	<b>ospfVirtIfStateChange</b>	1.3.6.1.2.1.14.16.2	6	1	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfNbrStateChange</b>	1.3.6.1.2.1.14.16.2	6	2	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfVirtNbrStateChange</b>	1.3.6.1.2.1.14.16.2	6	3	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfIfConfigError</b>	1.3.6.1.2.1.14.16.2	6	4	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfVirtIfConfigError</b>	1.3.6.1.2.1.14.16.2	6	5	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfIfAuthFailure</b>	1.3.6.1.2.1.14.16.2	6	6	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfVirtIfAuthFailure</b>	1.3.6.1.2.1.14.16.2	6	7	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfIfRxBadPacket</b>	1.3.6.1.2.1.14.16.2	6	8	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfVirtIfRxBadPacket</b>	1.3.6.1.2.1.14.16.2	6	9	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfTxRetransmit</b>	1.3.6.1.2.1.14.16.2	6	10	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfVirtIfTxRetransmit</b>	1.3.6.1.2.1.14.16.2	6	11	–	–	M, T, MX, J, EX, and SRX for branch devices.
	<b>ospfMaxAgeLsa</b>	1.3.6.1.2.1.14.16.2	6	13	–	–	M, T, MX, J, EX, and SRX for branch devices.

Table 270: Standard Supported SNMP Version 1 Traps (*continued*)

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag	Supported On
	<b>ospflfStateChange</b>	1.3.6.1.2.1.14.16.2	6	16	–	–	M, T, MX, J, EX, and SRX for branch devices.
<b>VRRP Notifications</b>							
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i>	<b>vrpTrapNewMaster</b>	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW_MASTER_TRAP	All devices running Junos OS.
	<b>vrpTrapAuthFailure</b>	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_FAILURE_TRAP	All devices running Junos OS.
RFC 6527, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)</i>	<b>vrpvp3NewMaster</b>	1.3.6.1.2.1.207	6	1	Warning	VRRPD_NEW_MASTER	M and MX
	<b>vrpvp3ProtoError</b>	1.3.6.1.2.1.207	6	2	Warning	VRRPD_V3_PROTO_ERROR	M and MX

#### Related Documentation

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Managing Traps and Informs on page 1981](#)

#### Standard SNMP Version 2 Traps

[Table 271 on page 1888](#) provides an overview of the standard SNMPv2 traps supported by the Junos OS. The traps are organized first by trap category and then by trap name and include their **snmpTrapOID**. The system logging severity levels are listed for those traps that have them with their corresponding system log tag. Traps that do not have corresponding system logging severity levels are marked with an en dash (–) in the table.

For more information about system log messages, see *System Log Monitoring and Troubleshooting Guide for Security Devices*.

Table 271: Standard Supported SNMP Version 2 Traps

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
<b>Startup Notifications</b>					
RFC 1907, <i>Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	<b>coldStart</b>	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_COLD_START	All devices running Junos OS.
	<b>warmStart</b>	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START	All devices running Junos OS.
	<b>authenticationFailure</b>	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_GEN_FAILURE	All devices running Junos OS.
<b>Link Notifications</b>					
RFC 2863, <i>The Interfaces Group MIB</i>	<b>linkDown</b>	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_LINK_DOWN	All devices running Junos OS.
	<b>linkUp</b>	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_LINK_UP	All devices running Junos OS.
<b>Remote Operations Notifications</b>					
RFC 2925, <i>Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i>	<b>pingProbeFailed</b>	1.3.6.1.2.1.80.0.1	Info	SNMP_TRAP_PING_PROBE_FAILED	All devices running Junos OS.
	<b>pingTestFailed</b>	1.3.6.1.2.1.80.0.2	Info	SNMP_TRAP_PING_TEST_FAILED	All devices running Junos OS.
	<b>pingTestCompleted</b>	1.3.6.1.2.1.80.0.3	Info	SNMP_TRAP_PING_TEST_COMPLETED	All devices running Junos OS.
	<b>traceRoutePathChange</b>	1.3.6.1.2.1.81.0.1	Info	SNMP_TRAP_TRACE_ROUTE_PATH_CHANGE	All devices running Junos OS.
	<b>traceRouteTestFailed</b>	1.3.6.1.2.1.81.0.2	Info	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED	All devices running Junos OS.
	<b>traceRouteTestCompleted</b>	1.3.6.1.2.1.81.0.3	Info	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED	All devices running Junos OS.
<b>RMON Alarms</b>					
RFC 2819a, <i>RMON MIB</i>	<b>fallingAlarm</b>	1.3.6.1.2.1.16.0.1	–	–	All devices running Junos OS.
	<b>risingAlarm</b>	1.3.6.1.2.1.16.0.2	–	–	All devices running Junos OS.

Table 271: Standard Supported SNMP Version 2 Traps (*continued*)

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
Routing Notifications					
<i>BGP 4 MIB</i>	<b>bgpEstablished</b>	1.3.6.1.2.1.15.7.1	–	–	All devices running Junos OS.
	<b>bgpBackwardTransition</b>	1.3.6.1.2.1.15.7.2	–	–	All devices running Junos OS.
<i>OSPF Trap MIB</i>	<b>ospfVirtIfStateChange</b>	1.3.6.1.2.1.14.16.2.1	–	–	All devices running Junos OS.
	<b>ospfNbrStateChange</b>	1.3.6.1.2.1.14.16.2.2	–	–	All devices running Junos OS.
	<b>ospfVirtNbrStateChange</b>	1.3.6.1.2.1.14.16.2.3	–	–	All devices running Junos OS.
	<b>ospfIfConfigError</b>	1.3.6.1.2.1.14.16.2.4	–	–	All devices running Junos OS.
	<b>ospfVirtIfConfigError</b>	1.3.6.1.2.1.14.16.2.5	–	–	All devices running Junos OS.
	<b>ospfIfAuthFailure</b>	1.3.6.1.2.1.14.16.2.6	–	–	All devices running Junos OS.
	<b>ospfVirtIfAuthFailure</b>	1.3.6.1.2.1.14.16.2.7	–	–	All devices running Junos OS.
	<b>ospfIfRxBadPacket</b>	1.3.6.1.2.1.14.16.2.8	–	–	All devices running Junos OS.
	<b>ospfVirtIfRxBadPacket</b>	1.3.6.1.2.1.14.16.2.9	–	–	All devices running Junos OS.
	<b>ospfTxRetransmit</b>	1.3.6.1.2.1.14.16.2.10	–	–	All devices running Junos OS.
	<b>ospfVirtIfTxRetransmit</b>	1.3.6.1.2.1.14.16.2.11	–	–	All devices running Junos OS.
	<b>ospfMaxAgeLsa</b>	1.3.6.1.2.1.14.16.2.13	–	–	All devices running Junos OS.
	<b>ospfIfStateChange</b>	1.3.6.1.2.1.14.16.2.16	–	–	All devices running Junos OS.
VRRP Notifications					

Table 271: Standard Supported SNMP Version 2 Traps (*continued*)

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
RFC 2787, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol</i>	<b>vrpTrapNewMaster</b>	1.3.6.1.2.1.68.0.1	Warning	VRRPD_NEWMASTER_TRAP	All devices running Junos OS.
	<b>vrpTrapAuthFailure</b>	1.3.6.1.2.1.68.0.2	Warning	VRRPD_AUTH_FAILURE_TRAP	All devices running Junos OS.
RFC 6527, <i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)</i>	<b>vrpv3NewMaster</b>	1.3.6.1.2.1.207.0.1	Warning	VRRPD_NEW_MASTER	M and MX
	<b>vrpv3ProtoError</b>	1.3.6.1.2.1.207.0.2	Warning	VRRPD_V3_PROTO_ERROR	M and MX

The Junos OS also supports the following standard SNMP version 2 traps:

- [SNMP Version 2 MPLS Traps on page 1890](#)

#### **SNMP Version 2 MPLS Traps**

The Junos OS supports the MPLS SNMP version 2 traps defined in RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base*.

You can disable the MPLS traps by including the **no-trap** option at the **[edit protocol mpls log-updown]** hierarchy level. For information about disabling the generation of MPLS traps, see the *Junos OS MPLS Applications Configuration Guide*.

The Junos OS supports the following MPLS traps:

- **mplsTunnelUp**—Generated when an **mplsTunnelOperStatus** object for one of the configured tunnels leaves the **down** state and transitions into another state, other than the **notPresent** state.
- **mplsTunnelDown**—Generated when an **mplsTunnelOperStatus** object for one of the configured tunnels enters the **down** state from a state other than the **notPresent** state.



**NOTE:** When an LSP flaps, only the ingress and egress routers of that LSP generate the **mplsTunnelUp** and **mplsTunnelDown** traps. Previously, all the routers associated with an LSP—that is, the ingress, egress, and transit routers—used to generate the traps when the LSP flaps.



- **mplsTunnelRerouted**—Generated when a tunnel is rerouted.
- **mplsTunnelReoptimized**—Generated when a tunnel is reoptimized.



**NOTE:** In Junos OS Release 8.3 and earlier, **mplsTunnelReoptimized** was generated every time the optimization timer expired; that is, when the optimization timer exceeded the value set for the **optimize-timer** statement at the **[edit protocols mpls label-switched-path path-name]** hierarchy level. However, in Release 8.4 and later, this trap is generated only when the path is reoptimized, and not when the optimization timer expires.

The Junos OS also supports the following L3VPN SNMP version 2 traps defined in RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN)*:

- **mplsL3VpnVrfUp**—Generated when:
  - No interface is associated with this VRF, and the first (and only first) interface associated with it has its **ifOperStatus** change to **up**.
  - Only one interface is associated with this VRF, and the **ifOperStatus** of this interface changes to **up**.
  - Multiple interfaces are associated with this VRF, and the **ifOperStatus** of all interfaces is **down**, and the first of those interfaces has its **ifOperStatus** change to **up**.
- **mplsL3VpnVrfDown**—Generated when:
  - One interface is associated with this VRF, and the **ifOperStatus** of this interface changes from **up** to **down**.
  - Multiple interfaces are associated with this VRF, and the **ifOperStatus** of all except one of these interfaces is equal to **up**, and the **ifOperStatus** of that interface changes from **up** to **down**.
  - The last interface with **ifOperStatus** equal to **up** is disassociated from a VRF.
- **mplsL3VpnVrfRouteMidThreshExceeded**—Generated when the number of routes contained by the specified VRF exceeds the value indicated by **mplsL3VpnVrfMidRouteThreshold**.
- **mplsL3VpnVrfNumVrfRouteMaxThreshExceeded**—Generated when the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by **mplsL3VpnVrfMaxRouteThreshold**.
- **mplsL3VpnNumVrfSecIlglLblThrshExcd**—Generated when the number of illegal label violations on a VRF as indicated by **mplsL3VpnVrfSecIllegalLblVltnsh** has exceeded **mplsL3VpnIlglLblRcvThrsh**.
- **mplsL3VpnNumVrfRouteMaxThreshCleared**—Generated only after the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by **mplsVrfMaxRouteThreshold**, and then falls below this value.

**Related  
Documentation**

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1804](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Managing Traps and Informs on page 1981](#)

---

### **Unsupported Standard SNMP Traps**

Standard SNMP traps that are defined in MIBs supported by the Junos OS but are not generated by the Junos OS are shown in [Table 272 on page 1893](#).

Table 272: Unsupported Standard SNMP Traps

MIB	Trap Name	Description
isismib.mib	isisDatabaseOverload	Generated when the system enters or leaves the overload state.
	isisManualAddressDrops	Generated when one of the manual <b>areaAddresses</b> assigned to the system is ignored when computing routes.
	isisCorruptedLSPDetected	Generated when an LSP stored in memory becomes corrupted.
	isisAttemptToExceedMaxSequence	Generated when the sequence number on a generated LSP wraps the 32-bit sequence counter and the number is purged.
	isisIDLenMismatch	Generated when a protocol data unit (PDU) is received with a different value for the system ID length. This trap includes an index to identify the circuit where the PDU was received and the PDU header.
	isisMaxAreaAddressesMismatch	Generated when a PDU with a different value for the maximum area addresses is received.
	isisOwnLSPPurge	Generated when a PDU is received with a system ID and zero age. This notification includes the circuit index if available.
	isisSequenceNumberSkip	Generated when an LSP is received with a system ID and different contents, indicating the LSP might require a higher sequence number.
	isisAuthenticationTypeFailure	Generated when a PDU with the wrong authentication type field is received.
	isisAuthenticationFailure	Generated when a PDU with an incorrect authentication information field is received.
	isisVersionSkew	Generated when a hello PDU from an IS running a different version of the protocol is received.
	isisAreaMismatch	Generated when a hello PDU from an IS which does not share any area address is received.
	isisRejectedAdjacency	Generated when a hello PDU from an IS is received, but no adjacency is established because of a lack of resources.
	isisLSPTooLargeToPropagate	Generated when a link-state PDU that is larger than the <b>dataLinkBlockSize</b> for a circuit is attempted, but not propagated.
	isisOriginatingLSPBufferSizeMismatch	

Table 272: Unsupported Standard SNMP Traps (*continued*)

MIB	Trap Name	Description
l3vpn-mib.mib		Generated when a Level 1 link-state PDU or Level 2 link-state PDU is received that is larger than the local value for originating <b>L1LSPBufferSize</b> or originating <b>L2LSPBufferSize</b> , respectively, or when a Level 1 link-state PDU or Level 2 link-state PDU is received containing the originating <b>LSPBufferSize</b> option and the value in the PDU option field does not match the local value for originating <b>L1LSPBufferSize</b> or originating <b>L2LSPBufferSize</b> , respectively.
	<b>isisProtocolsSupportedMismatch</b>	Generated when a nonpseudonode, segment 0 link-state PDU is received that has no matching protocols.
	<b>mplsVrflfUp</b>	Generated when the <b>ifOperStatus</b> of an interface associated with a VRF table changes to the <b>up(1)</b> state, or when an interface with <b>ifOperStatus = up(1)</b> is associated with a VRF table.
	<b>mplsVrflfDown</b>	Generated when the <b>ifOperStatus</b> of an interface associated with a VRF table changes to the <b>down(1)</b> state, or when an interface with <b>ifOperStatus = up(1)</b> state is disassociated from a VRF table.
	<b>mplsNumVrfRouteMidThreshExceeded</b>	Generated when the number of routes contained by the specified VRF table exceeds the value indicated by <b>mplsVrfMidRouteThreshold</b> .
msdpmib.mib	<b>mplsNumVrfRouteMaxThreshExceeded</b>	Generated when the number of routes contained by the specified VRF table reaches or attempts to exceed the maximum allowed value as indicated by <b>mplsVrfMaxRouteThreshold</b> .
	<b>mplsNumVrfSecIllegalLblThrshExcd</b>	Generated when the number of illegal label violations on a VRF table as indicated by <b>mplsVpnVrfSecIllegalLblVltns</b> has exceeded <b>mplsVpnVrfSecIllegalLblRcvThrsh</b> .
ospf2trap.mib	<b>msdpEstablished</b>	Generated when the Multicast Source Discovery Protocol (MSDP) finite state machine (FSM) enters the <b>Established</b> state.
	<b>msdpBackwardTransition</b>	Generated when the MSDP FSM moves from a higher numbered state to a lower numbered state.
ospf2trap.mib	<b>ospfOriginateLsa</b>	Generated when a new LSA is originated by the router because of a topology change.
	<b>ospfLsdbOverflow</b>	Generated when the number of LSAs in the router's link-state database exceeds the value of <b>ospfExtLsdbLimit</b> .
	<b>ospfLsdbApproachingOverflow</b>	Generated when the number of LSAs in the router's link-state database exceeds 90% of the value of <b>ospfExtLsdbLimit</b> .

Table 272: Unsupported Standard SNMP Traps (*continued*)

MIB	Trap Name	Description
rfc1747.mib	sdlcPortStatusChange	Generated when the state of an SDLC port transitions to active or inactive.
	sdlcLSStatusChange	Generated when the state of an SDLC link station transitions to contacted or disconnected.
rfc2115a.mib	frDLCIStatusChange	Generated when a virtual circuit changes state (has been created or invalidated, or has toggled between the active and inactive states).
rfc2662.mib	adslAtucRateChangeTrap	Generated when the ATUCs transmit rate has changed (RADSL mode only).
	adslAtucPerfLofsThreshTrap	Generated when the loss of framing 15-minute interval threshold is reached.
	adslAtucInitFailureTrap	Generated when ATUC initialization fails.
	adslAturPerfLprsThreshTrap	Generated when the loss of power 15-minute interval threshold is reached.
	adslAturRateChangeTrap	Generated when the ATURs transmit rate changes (RADSL mode only).
rfc3020.mib	mfrMibTrapBundleLinkMismatch	Generated when a bundle link mismatch is detected.
rfc3813.mib	mplsXCUp	Generated when <b>mplsXCOperStatus</b> for one or more contiguous entries in <b>mplsXCTable</b> enters the <b>up(1)</b> state from some other state.
	mplsXCDown	Generated when <b>mplsXCOperStatus</b> for one or more contiguous entries in <b>mplsXCTable</b> enters the <b>down(2)</b> state from some other state.

- Related Documentation**
- [Juniper Networks Enterprise-Specific SNMP Traps on page 1868](#)
  - [Standard SNMP Traps Supported on Devices Running Junos OS on page 1883](#)
  - [Juniper Networks Enterprise-Specific MIBs on page 1819](#)
  - [Standard SNMP MIBs Supported by Junos OS on page 1804](#)

## Loading MIB Files to a Network Management System

- [Loading MIB Files to a Network Management System on page 1895](#)

### 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 **Enterprise-Specific MIBs and Traps** section of the Junos OS Technical Publications index page at <http://www.juniper.net/techpubs/software/junos/index.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 Technical Publications index page (<http://www.juniper.net/techpubs/software/junos/index.html>).
2. Click the tab that corresponds to the Junos OS Release for which you want to download the MIB files.
3. On the selected tab, click the + (plus) sign that corresponds to the **Enterprise-Specific MIBs and Traps** section to expand the section.
4. Click the **TAR** or **ZIP** link that corresponds to the **Enterprise MIBs** link under the **Enterprise-Specific MIBs and Traps** section to download the Junos MIB package.
5. Decompress the file (**.tar** or **.zip**) using an appropriate utility.
6. 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**

7. 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.

8. 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

9. 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 1804](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1819](#)

## Configuring SNMP

- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1900](#)
- [Configuring the System Location for a Device Running Junos OS on page 1900](#)
- [Configuring the System Description on a Device Running Junos OS on page 1901](#)
- [Configuring the System Name on page 1901](#)
- [Configuring the Commit Delay Timer on page 1902](#)
- [Configuring the SNMP Community String on page 1902](#)

- [Examples: Configuring the SNMP Community String on page 1903](#)
- [Filtering Duplicate SNMP Requests on page 1904](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1905](#)
- [Example: Configuring Secured Access List Checking on page 1905](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1905](#)
- [Configuring MIB Views on page 1906](#)
- [Example: Ping Proxy MIB on page 1907](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Configuring SNMP Trap Options on page 1909](#)
- [Configuring SNMP Trap Groups on page 1912](#)
- [Example: Configuring SNMP Trap Groups on page 1914](#)
- [Configuring the Trap Notification Filter on page 1915](#)

---

### Configuring SNMP on a Device Running Junos OS

By default, SNMP is disabled on devices running Junos OS. To enable SNMP on a router or switch, you must include the SNMP configuration statements at the **[edit snmp]** hierarchy level.

To configure the minimum requirements for SNMP, include the following statements at the **[edit snmp]** hierarchy level of the configuration:

```
[edit]
snmp {
 community public;
}
```

The community defined here as **public** grants read access to all MIB data to any client.

To configure complete SNMP features, include the following statements at the **[edit snmp]** hierarchy level:

```
snmp {
 client-list client-list-name {
 ip-addresses;
 }
 community community-name {
 authorization authorization;
 client-list-name client-list-name;
 clients {
 address restrict;
 }
 routing-instance routing-instance-name {
 clients {
 addresses;
 }
 }
 }
 logical-system logical-system-name {
 routing-instance routing-instance-name {
 clients {
 addresses;
 }
 }
 }
}
```



```

 }
 }
}
view view-name;
}
contact contact;
description description;
engine-id {
 (local engine-id | use-mac-address | use-default-ip-address);
}
filter-duplicates;
health-monitor {
 falling-threshold integer;
 interval seconds;
 rising-threshold integer;
}
interface [interface-names];
location location;
name name;
nonvolatile {
 commit-delay seconds;
}
rmon {
 alarm index {
 description text-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;
 sample-type type;
 startup-alarm alarm;
 syslog-subtag syslog-subtag;
 variable oid-variable;
 }
 event index {
 community community-name;
 description text-description;
 type type;
 }
}
traceoptions {
 file filename <files number> <size size> <world-readable | no-world-readable> <match
 regular-expression>;
 flag flag;
}
trap-group group-name {
 categories {
 category;
 }
 destination-port port-number;
 routing-instance instance;
 targets {
 address;
 }
}

```

```
 version (all | v1 | v2);
 }
 trap-options {
 agent-address outgoing-interface;
 source-address address;
 }
 view view-name {
 oid object-identifier (include | exclude);
 }
}
```

**Related Documentation**

- [Understanding the SNMP Implementation in Junos OS on page 1800](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)

---

### 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 on page 1898](#)
- [Configuring the System Location for a Device Running Junos OS on page 1900](#)
- [Configuring the System Description on a Device Running Junos OS on page 1901](#)
- [Configuring the System Name on page 1901](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

---

### 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 on page 1898](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1900](#)
- [Configuring the System Description on a Device Running Junos OS on page 1901](#)
- [Configuring the System Name on page 1901](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

---

### 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 on page 1898](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1900](#)
- [Configuring the System Location for a Device Running Junos OS on page 1900](#)
- [Configuring the System Name on page 1901](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

---

### Configuring the 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 "snmp 1";
}
```

**Related  
Documentation**

- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1900](#)
- [Configuring the System Location for a Device Running Junos OS on page 1900](#)
- [Configuring the System Description on a Device Running Junos OS on page 1901](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

### 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 on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

### Configuring the SNMP Community String

---

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 configure a community string in a Junos OS configuration, include the **community** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
 community name {
 authorization authorization;
 clients {
 default restrict;
 address restrict;
```

```

 }
 view view-name;
 }

```

If the community name contains spaces, enclose it in quotation marks (" ").

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 1906](#).

The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. If no **clients** statement is present, all clients are allowed. For **address**, you must specify an IPv4 or IPv6 address, not a hostname. Include the **default restrict** option to deny access to all SNMP clients for which access is not explicitly granted. We recommend that you always include the **default restrict** option to limit SNMP client access to the local router.



**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.

#### Related Documentation

- [Adding a Group of Clients to an SNMP Community on page 1944](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Examples: Configuring the SNMP Community String on page 1903](#)

#### 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 the SNMP Community String on page 1902](#)

### 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 on page 1898](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1905](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1905](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

### 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 on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Example: Configuring Secured Access List Checking on page 1905](#)
- [Configuring SNMP](#)

### 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 1905](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1905](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

### 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 {
 interface1;
 interface2;
 }
 all-internal-interfaces;
 }
}
```

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 1905](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

---

### Configuring MIB Views

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

- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Example: Ping Proxy MIB on page 1907](#)
- [view \(Configuring a MIB View\) on page 2088](#)
- [view \(Associating MIB View with a Community\)](#)
- [oid on page 2046](#)

#### 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 on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

- [Configuring MIB Views on page 1906](#)
- [view \(Configuring a MIB View\) on page 2088](#)
- [oid on page 2046](#)

### [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 1909](#)
- [Configuring SNMP Trap Groups on page 1912](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

## 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 1912](#).

This topic contains the following sections:

- [Configuring the Source Address for SNMP Traps on page 1909](#)
- [Configuring the Agent Address for SNMP Traps on page 1911](#)
- [Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps on page 1912](#)

### Configuring the Source Address for SNMP Traps

You can configure the source address of trap packets in many ways: **lo0**, a valid IPv4 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**.

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
- **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 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.

**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 used 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 1908](#)
- [Configuring SNMP Trap Groups on page 1912](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

### 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 1883 and “Juniper Networks Enterprise-Specific SNMP Traps” on page 1868 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
- **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](#).

#### Related Documentation

- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Configuring SNMP Trap Options on page 1909](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Example: Configuring SNMP Trap Groups on page 1914](#)

#### 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 1912](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1908](#)
- [Configuring SNMP Trap Options on page 1909](#)

### 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 1936](#)
- [Configuring the SNMPv3 Trap Notification on page 1937](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Defining and Configuring the Trap Target Parameters on page 1941](#)
- [Configuring SNMP Informs on page 1935](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

## Configuring SNMPv3

- [SNMPv3 Overview on page 1916](#)
- [Creating SNMPv3 Users on page 1917](#)
- [Example: SNMPv3 Configuration on page 1918](#)
- [Example: Creating SNMPv3 Users Configuration on page 1921](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Configuring the SNMPv3 Authentication Type on page 1923](#)
- [Configuring the Encryption Type on page 1925](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring the Access Privileges Granted to a Group on page 1928](#)
- [Example: Access Privilege Configuration on page 1931](#)
- [Assigning Security Model and Security Name to a Group on page 1932](#)
- [Example: Security Group Configuration on page 1933](#)
- [Example: Configuring the Tag List on page 1934](#)
- [Configuring the Local Engine ID on page 1934](#)
- [Configuring SNMP Informs on page 1935](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring the SNMPv3 Trap Notification on page 1937](#)
- [Example: Configuring SNMPv3 Trap Notification on page 1938](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Defining and Configuring the Trap Target Parameters on page 1941](#)
- [Adding a Group of Clients to an SNMP Community on page 1944](#)
- [Configuring the SNMPv3 Community on page 1945](#)
- [Example: SNMPv3 Community Configuration on page 1947](#)
- [Configuring the Inform Notification Type and Target Address on page 1948](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1949](#)
- [Configuring the Remote Engine and Remote User on page 1950](#)
- [Example: Configuring the Remote Engine ID and Remote Users on page 1951](#)
- [Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage on page 1951](#)

---

### 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 1917](#)
- [Configuring MIB Views on page 1906](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring SNMP Informs on page 1935](#)

#### Related Documentation

- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: Creating SNMPv3 Users Configuration on page 1921](#)
- [Example: SNMPv3 Configuration on page 1918](#)

---

### 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 "$ABC123"; # 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 2007](#)
  - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### Example: Creating SNMPv3 Users Configuration

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 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 1917](#)
- [Configuring MIB Views on page 1906](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring SNMP Informs on page 1935](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Example: SNMPv3 Configuration on page 1918](#)

#### 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 1924](#)
- [Configuring SHA Authentication on page 1924](#)
- [Configuring No Authentication on page 1924](#)

### 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 Encryption Type on page 1925](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring the Access Privileges Granted to a Group on page 1928](#)
- [Assigning Security Model and Security Name to a Group on page 1932](#)

- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### Configuring the 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 1925](#)
- [Configuring the Data Encryption Algorithm on page 1925](#)
- [Configuring Triple DES on page 1926](#)
- [Configuring No Encryption on page 1926](#)

#### 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 1923](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring the Access Privileges Granted to a Group on page 1928](#)
- [Assigning Security Model and Security Name to a Group on page 1932](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

---

### **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 1906](#).

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 1923](#)

- [Configuring the Access Privileges Granted to a Group on page 1928](#)
- [Assigning Security Model and Security Name to a Group on page 1932](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

---

## Configuring the Access Privileges Granted to a Group

This topic includes the following sections:

- [Configuring the Group on page 1928](#)
- [Configuring the Security Model on page 1928](#)
- [Configuring the Security Level on page 1928](#)
- [Associating MIB Views with an SNMP User Group on page 1929](#)

### 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 1906](#).

This section describes the following topics related to this configuration:

- [Configuring the Notify View on page 1930](#)
- [Configuring the Read View on page 1930](#)
- [Configuring the Write View on page 1930](#)

### 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 1923](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Assigning Security Model and Security Name to a Group on page 1932](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: Access Privilege Configuration on page 1931](#)



### Example: Access Privilege Configuration

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 1928](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

## 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 1932](#)
- [Assigning Security Names to Groups on page 1932](#)
- [Configuring the Group on page 1933](#)

### 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 1917](#). For information about configuring a community string, see [“Configuring the SNMPv3 Community” on page 1945](#).



**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 1926](#).

---

### **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 1932](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 1936](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: SNMPv3 Configuration on page 1918](#)

### 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:

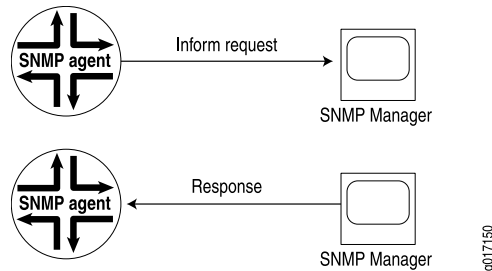
- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.
- A specified number of unsuccessful retransmissions have been attempted and the agent discards the inform message.

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 60 on page 1936](#)). 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 60: Inform Request and Response**



For information about configuring SNMP traps, see [“Configuring SNMPv3 Traps on a Device Running Junos OS” on page 1936](#).

#### Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring the Remote Engine and Remote User on page 1950](#)
- [Configuring the Inform Notification Type and Target Address on page 1948](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 1935](#).

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 1937](#)
- [Configuring the Trap Notification Filter on page 1915](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Defining and Configuring the Trap Target Parameters on page 1941](#)
- [Configuring SNMP Informs on page 1935](#)
- [Configuring the Remote Engine and Remote User on page 1950](#)
- [Configuring the Inform Notification Type and Target Address on page 1948](#)

### 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 1940.

**Related  
Documentation**

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring the Trap Notification Filter on page 1915](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Defining and Configuring the Trap Target Parameters on page 1941](#)
- [Configuring SNMP Informs on page 1935](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

---

### 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 1936](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)



## 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 1939](#)
- [Configuring the Address Mask on page 1940](#)
- [Configuring the Port on page 1940](#)
- [Configuring the Routing Instance on page 1940](#)
- [Configuring the Trap Target Address on page 1940](#)
- [Applying Target Parameters on page 1941](#)

### 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 1945](#).

### 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 1934](#).

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 1937.



**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 1936](#)
- [Configuring the SNMPv3 Trap Notification on page 1937](#)
- [Configuring the Trap Notification Filter on page 1915](#)
- [Defining and Configuring the Trap Target Parameters on page 1941](#)
- [Configuring SNMP Informs on page 1935](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)

### 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 1942](#)
- [Configuring the Target Parameters on page 1942](#)

#### ***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 1915.

#### ***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 1942](#)
- [Configuring the Security Model on page 1943](#)
- [Configuring the Security Level on page 1943](#)
- [Configuring the Security Name on page 1943](#)

#### ***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 1936](#)
- [Configuring the SNMPv3 Trap Notification on page 1937](#)
- [Configuring the Trap Notification Filter on page 1915](#)
- [Configuring the Trap Target Address on page 1939](#)
- [Configuring SNMP Informs on page 1935](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 Policy Configuration Guide*.

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 clientlist1 {
 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 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 1946](#)
- [Configuring the Context on page 1946](#)
- [Configuring the Security Names on page 1947](#)
- [Configuring the Tag on page 1947](#)

### 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]
tagtag-name;
```

**tag-name** identifies the address of managers that are allowed to use a community string.

#### Related Documentation

- [Creating SNMPv3 Users on page 1917](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: SNMPv3 Community Configuration on page 1947](#)

### Example: SNMPv3 Community Configuration

Define an SNMP community:

```
[edit snmp v3]
snmp-community index1 {
 community-name "$ABC123"; # 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 1945](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)

- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 1940](#).

**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 1936](#)
- [Configuring SNMP Informs on page 1935](#)
- [Configuring the Remote Engine and Remote User on page 1950](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1949](#)

---

### 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 1948](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

### 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 1936](#)
- [Configuring SNMP Inform on page 1935](#)
- [Configuring the Inform Notification Type and Target Address on page 1948](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)
- [Example: Configuring the Remote Engine ID and Remote Users on page 1951](#)

---

### Example: Configuring the Remote Engine ID and Remote Users

The following example configures user **u10** located on remote engine **0x800007E5804089071BC6D10A41** and the user's authentication and privacy keys. The keys are autogenerated from the passwords entered by the command-line interface (CLI) user.

```
[edit snmp v3]
usm {
 remote-engine 800007E5804089071BC6D10A41 {
 user u10 {
 authentication-md5 {
 authentication-key "$ABC123"
 }
 }
 privacy-des {
 privacy-key "$ABC123"
 }
 }
}
```

**Related Documentation**

- [Configuring the Remote Engine and Remote User on page 1950](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

---

### Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage

Even though Junos OS includes built-in performance metrics and monitoring options, you might need to have customized performance metrics. To make it easier for you to monitor such customized data through a standard monitoring system, Junos OS provides you with an enterprise-specific Utility MIB that can store such data and thus extend SNMP support for managing and monitoring the data of your choice.

The enterprise-specific Utility MIB provides you with container objects of the following types: **32-bit counters**, **64-bit counters**, **signed integers**, **unsigned integers**, and **octet strings**.

You can use these container MIB objects to store the data that are otherwise not supported for SNMP operations. You can populate data for these objects either by using CLI commands or with the help of Op scripts and an RPC API that can invoke the CLI commands.

The following CLI commands enable you to set and clear Utility MIB object values:

- **request snmp utility-mib set** instance *name* object-type <counter | counter 64 | integer | string | unsigned integer> object-value *value*
- **request snmp utility-mib clear** instance *name* object-type <counter | counter 64 | integer | string | unsigned integer>

The *instance name* option of the **request snmp utility-mib <set | clear>** command specifies the name of the data instance and is the main identifier of the data. The **object-type <counter | counter 64 | integer | string | unsigned integer>** option enables you specify the object type, and the **object-value *value*** option enables you to set the value of the object.

To automate the process of populating Utility MIB data, you can use a combination of an event policy and event script. The following examples show the configuration for an event policy to run **show system buffers** every hour and to store the **show system buffers** data in Utility MIB objects by running an event script (**check-mbufs.slax**).

**Event Policy Configuration** To configure an event policy that runs the **show system buffers** command every hour and invokes **check-mbufs.slax** to store the **show system buffers** data into Utility MIB objects, include the following statements at the **[edit]** hierarchy level:

```
event-options {
 generate-event {
 1-HOUR time-interval 3600;
 }
 policy MBUFS {
 events 1-HOUR;
 then {
 event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
 }
 }
 event-script {
 file check-mbufs.slax;
 }
}
```

**check-mbufs.slax Script** The following example shows the **check-mbufs.slax** script that is stored under **/var/db/scripts/event/**:

```
----- script START -----
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";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
 <op-script-results>{
```

```

var $cmd = <command> "show system buffers";
var $out = jcs:invoke($cmd);

var $lines = jcs:break_lines($out);
for-each ($lines) {
 if (contains(., "current/peak/max")) {
 var $pattern = "([0-9]+)/([0-9]+)/([0-9]+) mbufs";
 var $split = jcs:regex($pattern, .);
 var $result = $split[2];

 var $rpc = <request-snmp-utility-mib-set> {
 <object-type> "integer";
 <instance> "current-mbufs";
 <object-value> $result;
 }
 var $res = jcs:invoke($rpc);
 }
}
}
----- script END -----

```

You can run the following command to check the data stored in the Utility MIB as a result of the event policy and script shown in the preceding examples:

```

user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs"
= 0 jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c 03 14 2c 00 2d 07 00
user@host>

```

#### Related Documentation

- [SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices](#)

## Configuring Routing Instances

- [Understanding SNMP Support for Routing Instances on page 1953](#)
- [Trap Support for Routing Instances on page 1954](#)
- [Identifying a Routing Instance on page 1955](#)
- [Enabling SNMP Access over Routing Instances on page 1956](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1957](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1959](#)

### 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.

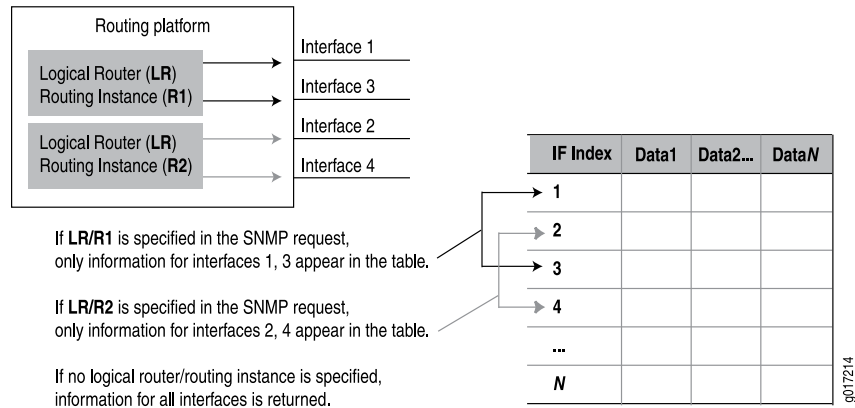
In Junos OS:

- 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 61 on page 1954](#)). Service providers can use this information for their own management needs or export the data for use by their customers.

**Figure 61: 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

- [Trap Support for Routing Instances on page 1954](#)
- [Identifying a Routing Instance on page 1955](#)
- [Enabling SNMP Access over Routing Instances on page 1956](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1959](#)

#### Trap Support 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 1953](#)
- [MIB Support Details on page 1851](#)

---

### 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 on page 1953](#)
- [Enabling SNMP Access over Routing Instances on page 1956](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)

### 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 1953](#)
- [Identifying a Routing Instance on page 1955](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1959](#)

### 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 1953](#)
- [Identifying a Routing Instance on page 1955](#)
- [Enabling SNMP Access over Routing Instances on page 1956](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1959](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1957](#)

#### 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]
INFrtid {
 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 **INFrtid** with the SNMP community **public**:

```

router# snmpwalk -Os router1 INFrtid@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 1953](#)
  - [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)

### 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 1953](#)
- [Enabling SNMP Access over Routing Instances on page 1956](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956](#)

### Configuring Remote Operations

- [SNMP Remote Operations Overview on page 1960](#)
- [Using the Ping MIB for Remote Monitoring Devices Running Junos OS on page 1962](#)
- [Starting a Ping Test on page 1963](#)
- [Monitoring a Running Ping Test on page 1964](#)
- [Gathering Ping Test Results on page 1967](#)
- [Stopping a Ping Test on page 1968](#)
- [Interpreting Ping Variables on page 1968](#)
- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1969](#)

## 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 1960](#)
- [Setting SNMP Views on page 1960](#)
- [Setting Trap Notification for Remote Operations on page 1961](#)
- [Using Variable-Length String Indexes on page 1961](#)
- [Enabling Logging on page 1962](#)

### 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, **jnxPingMIB**, Traceroute MIB, and **jnxTraceRouteMIB**, 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 the SNMP Community String” on page 1902](#) and [community](#).

For more information about the **view** statement, see [“Configuring MIB Views” on page 1906](#), [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 1912](#).

### *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 1969](#).

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 1962](#)
- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1969](#)

### **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 1960](#)
- [Starting a Ping Test on page 1963](#)
- [Monitoring a Running Ping Test on page 1964](#)
- [Gathering Ping Test Results on page 1967](#)



- [Stopping a Ping Test on page 1968](#)
- [Interpreting Ping Variables on page 1968](#)

### 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 1960](#).

There are two ways to start a ping test:

- [Using Multiple Set Protocol Data Units \(PDUs\) on page 1963](#)
- [Using a Single Set PDU on page 1963](#)

#### *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 1964
- [pingProbeHistoryTable](#) on page 1965
- [Generating Traps](#) on page 1966

#### *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 1965.

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 1912](#) and [“Example: Setting Trap Notification for Remote Operations” on page 1961](#).

### 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 1964](#). For more information about Ping MIB traps, see [“Generating Traps” on page 1966](#).

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 273 on page 1967](#).

**Table 273: 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 274 on page 1967](#).

**Table 274: Results in pingProbeHistoryTable: After the First Probe of the Second Test**

pingProbeHistoryIndex	Probe Result
12	Result of 12th probe from run 1

**Table 274: 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 275 on page 1968](#).

**Table 275: 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 1960](#)

### Tracing SNMP Activity

- [Tracing SNMP Activity on a Device Running Junos OS on page 1969](#)
- [Example: Tracing SNMP Activity on page 1973](#)

### 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 Monitoring and Troubleshooting Guide for Security Devices*.)
  - 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;
 no-remote-trace;
}
```

These statements are described in the following sections:

- [Configuring the Number and Size of SNMP Log Files on page 1970](#)
- [Configuring Access to the Log File on page 1971](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 1971](#)
- [Configuring the Trace Operations on page 1971](#)

### **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 276 on page 1972 describes the meaning of the SNMP tracing flags.

Table 276: SNMP Tracing Flags

Flag	Description	Default Setting
<b>all</b>	Log all operations.	Off
<b>configuration</b>	Log reading of the configuration at the <b>[edit snmp]</b> hierarchy level.	Off
<b>database</b>	Log events involving storage and retrieval in the events database.	Off
<b>events</b>	Log important events.	Off
<b>general</b>	Log general events.	Off
<b>interface-stats</b>	Log physical and logical interface statistics.	Off
<b>nonvolatile-set</b>	Log nonvolatile SNMP set request handling.	Off
<b>pdu</b>	Log SNMP request and response packets.	Off
<b>policy</b>	Log policy processing.	Off
<b>protocol-timeouts</b>	Log SNMP response timeouts.	Off
<b>routing-socket</b>	Log routing socket calls.	Off
<b>server</b>	Log communication with processes that are generating events.	Off
<b>subagent</b>	Log subagent restarts.	Off
<b>timer</b>	Log internal timer events.	Off
<b>varbind-error</b>	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 on page 1898](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Example: Tracing SNMP Activity on page 1973](#)
- [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 on page 1898](#)
- [Tracing SNMP Activity on a Device Running Junos OS on page 1969](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)

## Configuring Vital MIB Data

- [Understanding Vital MIB OID Data Collection on page 1973](#)
- [Generating Readable Raw OID Data Collections on page 1974](#)
- [Generating Raw MIB OID from a Policy on page 1975](#)
- [Generating Vital Data of Pre-Defined Group on page 1976](#)
- [Generating Vital Data from an Interface on page 1977](#)
- [Generating Vital Data from an IPsec VPN on page 1978](#)
- [Generating Vital Data from a NAT Rule on page 1979](#)
- [Generating Vital Data from an Operating Component on page 1980](#)
- [Generating Vital Data from a Screen on page 1980](#)

### Understanding Vital MIB OID Data Collection

---

MIB object identifier (OID) data is collected and configured for later use in reports. You can configure data collection duration (default is 3 days), dump file size limitation (default is 5 megabytes for branch SRX Series and 10 megabytes for high-end SRX Series), and disk storage limitation (default is 80 percent). The expired dump file is removed automatically. When the dump file exceeds the limited size, a new dump file is created and the old dump file is compressed. When disk utilization exceeds the storage limitation, data collection is skipped but is attempted the next time. If an issue should arise, then the collected data is examined to help identify its cause.

Once you enable a predefined group, the vital data of all OIDs in the group are periodically collected and analyzed. Only critical data is collected when CPU utilization exceeds 60 percent but is within 80 percent.

A maximum of 64 groups per OIDs are supported for branch SRX Series devices and a maximum of 128 groups per OIDs are supported for high-end SRX Series devices.

You can also collect raw MIB OID data. For the format of raw OID output, the first volume is 40 characters and the second volume is 30 characters in length. Any extra characters are stripped.



**TIP:** To make the dump file easily understood, we recommend that you configure short comments for each raw OID.

Use the **set system processes system-log-vital disable** command to manually disable the syslvd process (daemon). Disabling syslvd will not impact the existing data in the dump file. Once all configuration commands are removed, syslvd is disabled automatically. If syslvd is disabled in the middle of a collection, data from the current collection will be lost but data available in the current dump file is retained.

#### Related Documentation

- [Generating Raw MIB OID from a Policy on page 1975](#)
- [Generating Readable Raw OID Data Collections on page 1974](#)

### Generating Readable Raw OID Data Collections

You can use the **set system log-vital add oid comment “comment”** command to make raw object identifiers (OIDs) that are lengthy and unreadable easily understood.

```
[edit system]
log-vital {
 add oid {
 comment comment;
 }
}
```

The **OID** parameter can be formatted as `mib-table.index`. For example, `jnxOperating1MinLoadAvg.9.1.0.0` is an OID.

The “*comment*” parameter describes the OID. If “*comment*” is present, the comment instead of the OID is generated as the subject of the vital data.

For example, without the “*comment*” parameter, the output of the **set system log-vital add jnxJsPolicyNumber.0** command in the dump file is:

```
=====
jnxJsPolicyNumber.0 1
=====
```

With the “*comment*” parameter, the output of the **set system log-vital add jnxJsPolicyNumber.0 comment “Total Policy Number”** command in the dump file is:

```
=====
Total Policy Number 1
=====
```



**NOTE:** For OIDs that are temporarily unavailable, the string **NA** is generated for them and the system continues to get their values for every collection. In this case, the output displayed in the dump file is:

```
=====
Total Policy Number NA
=====
```

**Related Documentation** • [Generating Raw MIB OID from a Policy on page 1975](#)

### Generating Raw MIB OID from a Policy

You can generate a raw MIB OID from a policy. You can also monitor the session number associated with the policy and other policy MIB tables.

For example, consider a policy called **test**. Monitor the session number associated with the policy.

```
[edit]
 from-zone untrust to-zone trust {
 policy test {
 match {
 source-address any;
 destination-address any;
 application any;
 }
 then {
 permit;
 count;
 }
 }
}
```

To monitor a session number associated with a policy:

1. Identify the OID of the policy's session number.

```
user@host> show snmp mib walk jnxJsPolicyName | match test
jnxJsPolicyName.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
= test
```

In the above output, the index of the policy is 7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116; the policy name is test; and the MIB table name is jnxJsPolicyName.

2. With the index, verify that both the from-zone and the to-zone match the configuration. Enter the **show snmp mib get** command.

```
user@host> show snmp mib get
jnxJsPolicyFromZone.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
jnxJsPolicyFromZone.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
= untrust

user@host> show snmp mib get
jnxJsPolicyToZone.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
```

```
jnxJsPolicyToZone.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
= trust
```

3. Perform a mandatory from-zone and to-zone match check to avoid a scenario where there is a policy with the same name but the from-zone or the to-zone is different.
4. After performing both the from-zone and the to-zone match checks, ensure that 7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116 is the index of the policy called test in various policy MIB tables.
5. Monitor the session number using the following command:

```
[edit]
user@host# set system log-vital add
jnxJsPolicyStatsNumSessions.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
comment "sess num of policy test"
```

The output of the configuration is:

```
=====
sess num of policy test 100
=====
```

To monitor other policy MIB tables:

1. Combine a MIB table's name with the index.
2. Monitor the session setup rate for the test policy using the command:

```
[edit]
set system log-vital add
jnxJsPolicyStatsSessionRate.7.117.110.116.114.117.115.116.5.116.114.117.115.116.4.116.101.115.116
comment "sess setup rate of policy test"
```

The output of the configuration is:

```
=====
sess setup rate of policy test 233
=====
```

#### Related Documentation

- [Understanding Vital MIB OID Data Collection on page 1973](#)
- [Generating Readable Raw OID Data Collections on page 1974](#)

#### Generating Vital Data of Pre-Defined Group

You can use the **set system log-vital group [cluster-counter | idp | operating | storage | spu <spu-name> | screen <zone-name>** command to enable a pre-defined group.

```
[edit system]
group {
 operating;
 idp;
 storage;
 cluster-counter;
 screen;
 spu;
}
```



**NOTE:** The parameter for `spu-name` must be *fwdd*, *all*, *fpcy.picz* or *nodex.fpcy.picz*.

The pre-defined groups are operating, SPU, storage, IDP, screen, and cluster-counter. Once a group is enabled, all OIDs in the group are periodically collected and dumped.

The operating group includes state, temperature, current CPU utilization percentage, buffer utilization percentage, heap-utilization percentage, up time, average-load in the last 1 minute, 5 minutes, or 15 minutes, and buffer-pool utilization percentage in the control plane of each operating component in the system.

The IDP group includes IDP data plane memory usage, IDP session usage and policies loaded number.

The storage group includes storage utilization of directory `/var/log`.

The cluster-counter group includes current total session number, total CPS, IPv4 CPS, IPv6 CPS, current total IPv4 session number, and current total IPv6 session number of both node 0 and node 1.

The screen group includes screen statistics of a specified zone.

The SPU group includes CPU usage, memory usage, current flow session number, current CP session number, IPv4 session number, IPv6 session number, CP IPv4 session number, and CP IPv6 session number of the SPU.

#### Related Documentation

- [Generating Raw MIB OID from a Policy on page 1975](#)

#### Generating Vital Data from an Interface

You can monitor the statistics of interface `ge-0/0/0` by first obtaining the SNMP `ifIndex` from the interface.

```
user@host> show interfaces ge-0/0/0
```

```
Physical interface: ge-0/0/0, Enabled, Physical link is Up
 Interface index: 134, SNMP ifIndex: 509
```

In this output, the 509 value is the index of `ge-0/0/0` in the interface MIB table. By combining this index value with the interface MIB tables, the vital data of the interface can be periodically collected.

For example, combine the 509 index with the `ifInErrors` interface MIB table to collect the In-Error data of interface `ge-0/0/0` by using the following command:

```
[edit]
user@host# set system log-vital add ifInErrors.509 comment "In-Err of ge-0/0/0"
The output for the command is:
```

```
=====
```

```
In-Err of ge-0/0/0 100
=====
```

The following interface MIB tables can be used to collect vital data:

- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors

**Related  
Documentation**

- [Generating Raw MIB OID from a Policy on page 1975](#)
- [Generating Readable Raw OID Data Collections on page 1974](#)

---

### Generating Vital Data from an IPsec VPN

You can monitor the vital data of an IPsec VPN by first obtaining the index of the VPN in the IPsec VPN MIB table.

For example, consider the following below policy-based VPN configuration, where the name of the policy is test.

```
user@host> show configuration security policies
```

```
from-zone untrust to-zone trust {
 policy test {
 match {
 source-address any;
 destination-address any;
 application any;
 }
 then {
 permit {
 tunnel {
 ipsec-vpn ike-vpn;
 }
 }
 }
 }
}
```



```
}
```

To monitor the error statistics for the VPN, you must first obtain the index of the VPN in the IPsec VPN MIB table. You can obtain this value by using the command:

```
user@host> show snmp mib walk jnxJsIpSecTunPolicyName | match test
jnxJsIpSecTunPolicyName.1.4.2.2.2.1.2 = test
```

In the output, 1.4.2.2.1.2 is the index of the IPsec SA associated with the policy called test. By combining the index with various IPsec VPN MIB tables, you can monitor the statistics by using the following commands:

```
[edit]
user@host# set system log-vital add jnxIpSecTunMonReplayDropPkts.1.4.2.2.2.1.2 comment
"Anti-Replay drop number of VPN policy test"
user@host# set system log-vital add jnxIpSecTunMonBadHeaders.1.4.2.2.2.1.2 comment "Bad
Header number of VPN policy test"
```

#### Related Documentation

- [Generating Vital Data from a Screen on page 1980](#)

### Generating Vital Data from a NAT Rule

You can monitor the vital data from a NAT rule (in this example, r1) by first obtaining the MIB index of r1.

Consider the following source NAT configuration.

```
user@host> show configuration security nat

source {
 rule-set rs1 {
 from zone trust;
 to zone untrust;
 rule r1 {
 match {
 source-address 17.0.0.0/8;
 destination-address 0.0.0.0/0;
 }
 then {
 source-nat {
 interface;
 }
 }
 }
 }
}
```

To find the MIB index of r1, enter the following command:

```
[edit]
user@host# show snmp mib walk jnxJsNatRuleName | grep r1
jnxJsNatRuleName.2.114.49.1 = r1
```

The output shows that 2.114.49.1 is the MIB index of r1.

Therefore, by combining the index with NAT MIB table jnxJsNatRuleHits, the session number associated with NAT rule r1 can be monitored by using the command:

```
[edit]
user@host# set system log-vital add jnxJsNatRuleHits.2.114.49.1 comment "Number of sessions
on NAT rule r1"
```

#### Related Documentation

- [Generating Readable Raw OID Data Collections on page 1974](#)

### Generating Vital Data from an Operating Component

You can monitor the vital data of an operating component. For example, to monitor the temperature of the SPC component located at slot 3 of node 0, enter the following command:

```
user@host> show snmp mib walk jnxOperatingDescr | match "SPC @ 3"
```

```
jnxOperatingDescr.7.4.0.0 = node0 FPC: SRX5k SPC @ 3/*/*
jnxOperatingDescr.7.10.0.0 = node1 FPC: SRX5k SPC @ 3/*/*
```

In the output, the SPC index at slot 3 of node 0 in the operating MIB table is 7.4.0.0. By combining the 7.4.0.0 index with operating MIB table `jnxOperatingTemp`, the temperature of SPC at slot 3 of node 0 can be monitored by using the following command:

```
[edit]
user@host# set system log-vital add jnxOperatingTemp.7.4.0.0 comment "Temperature of node0
SPC-3"
```

#### Related Documentation

- [Generating Vital Data from a Screen on page 1980](#)

### Generating Vital Data from a Screen

The screen group collects all screen statistics of a specified zone. However, it can only collect some of the statistics rather than all statistics.

For example, consider the following screen configuration, where the number of UDP flood attacks in the untrust zone is to be monitored.

```
user@host> show configuration security screen
```

```
ids-option zone-syn-flood {
 tcp {
 syn-flood {
 timeout 20;
 }
 }
}
```

```
user@host> show configuration security zones
```

```
security-zone untrust {
 screen zone-syn-flood;
 ...
}
```

To monitor the number of UDP flood attacks, you must first obtain the index of the untrust zone in various screen MIB tables.

```
user@host> show snmp mib walk jnxJsScreenZoneName | match untrust
jnxJsScreenZoneName.117.110.116.114.117.115.116.0
= untrust
```

In the output, the string  
117.110.116.114.117.115.116.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 is the index of  
the untrust zone in the MIB table.

By combining the index with screen MIB table jnxJsScreenMonUdpFlood, the number  
can be monitored using the following command:

```
[edit]
user@host# set system log-vital add
jnxJsScreenMonUdpFlood.117.110.116.114.117.115.116.0
comment "Number of UDP flood attack"
```

#### Related Documentation

- [Generating Vital Data from a NAT Rule on page 1979](#)

## SNMP FAQs

- [Managing Traps and Informs on page 1981](#)

### Managing Traps and Informs

The following sections contain a few tips on managing SNMP notifications:

- [Generating Traps Based on SysLog Events on page 1981](#)
- [Filtering Traps Based on the Trap Category on page 1982](#)
- [Filtering Traps Based on the Object Identifier on page 1982](#)

#### Generating Traps Based on SysLog Events

Event policies can include an action that raises traps for events based on system log messages. This feature enables notification of an SNMP trap-based application when an important system log message occurs. You can convert any system log message, for which there is no corresponding trap, into a trap. If you are using network management system traps rather than system log messages to monitor your network, you can use this feature to ensure that you are notified of all the major events.

To configure a policy that raises a trap on receipt of an event, include the following statements at the **[edit event-options policy *policy-name*]** hierarchy level:

```
[edit event-options policy policy-name]
events [events];
then {
 raise-trap;
}
```

The following example shows the sample configuration for raising a trap for the event **ui\_mgd\_terminate**:

#### Generating Traps Based on SysLog Events

```
[edit event-options policy p1]
events ui_mgd_terminate;
then {
 raise-trap;
```

```
}
```

### *Filtering Traps Based on the Trap Category*

SNMP traps are categorized into many categories. The Junos OS provides a configuration option, **categories** at the **[edit snmp trap-group trap-group]** hierarchy level, that enables you to specify categories of traps that you want to receive on a particular host. You can 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;
 }
}
```

### *Filtering Traps Based on the Object Identifier*

The Junos OS also provides a more advanced filter option that enables you to filter out specific traps based on their object identifiers. You can use the **notify-filter** option to filter out a specific trap or a group of traps.

The following example shows the sample configuration for excluding Juniper Networks enterprise-specific configuration management traps (note that the SNMPv3 configuration also supports filtering of SNMPv1 and SNMPv2 traps as is shown in the following 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 tgl;
 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 nfl;
 }
 notify v2c_notify {
 type trap;
 tag tgl;
 }
 notify-filter nfl {
 oid .1.3.6.1.4.1.2636.4.5 exclude;
 oid .1 include;
 }
 snmp-community index1 {
 community-name "$ABC123"; ## SECRET-DATA
 security-name sn_v2c_trap;
 tag tgl;
 }
 view all {
 oid .1 include;
 }
}
```

**Related  
Documentation**

- *Understanding SNMP Implementation in the Junos OS*
- *Configuring SNMP on Devices Running the Junos OS*
- *Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running the Junos OS*
- *Optimizing the Network Management System Configuration for the Best Results*
- *Configuring Options on Managed Devices for Better SNMP Response Time*
- *Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage*

---

## Remote Monitoring (RMON) with SNMP

- [RMON Overview on page 1984](#)
- [Configuring RMON Alarms and Events on page 1986](#)
- [Monitoring RMON Alarms and Events on page 1993](#)

## RMON Overview

- [Understanding RMON Alarms on page 1984](#)
- [Understanding RMON Events on page 1985](#)

---

### 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 1984](#)
- [jnxRmonAlarmTable on page 1985](#)

#### **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](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 *SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices*.

#### Related Documentation

- [Understanding RMON Events on page 1985](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)

### 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 1985](#)

#### **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 1984](#)
- [Configuring an Event Entry and Its Attributes on page 1991](#)

## Configuring RMON Alarms and Events

- [Understanding RMON Alarms and Events Configuration on page 1986](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)
- [Configuring an Event Entry and Its Attributes on page 1991](#)
- [Example: Configuring an RMON Alarm and Event Entry on page 1992](#)
- [Example: Configuring Health Monitoring on page 1992](#)

### 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 1984](#)
- [Understanding RMON Events on page 1985](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)
- [Configuring an Event Entry and Its Attributes on page 1991](#)

### 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 1987](#)
- [Configuring the Description on page 1988](#)
- [Configuring the Falling Event Index or Rising Event Index on page 1988](#)
- [Configuring the Falling Threshold or Rising Threshold on page 1988](#)
- [Configuring the Interval on page 1989](#)
- [Configuring the Falling Threshold Interval on page 1989](#)
- [Configuring the Request Type on page 1989](#)
- [Configuring the Sample Type on page 1990](#)
- [Configuring the Startup Alarm on page 1990](#)
- [Configuring the System Log Tag on page 1990](#)
- [Configuring the Variable on page 1991](#)

#### 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, 1.3.6.1.2.1.2.1.2.1.10.1) 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 1986](#)
- [Understanding RMON Alarms on page 1984](#)
- [Understanding RMON Events on page 1985](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)

- [Example: Configuring an RMON Alarm and Event Entry on page 1992](#)

---

### 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 1986](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)
- [Configuring an Event Entry and Its Attributes on page 1991](#)

---

### 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 1998](#)

## Monitoring RMON Alarms and Events

- [Understanding RMON for Monitoring Service Quality on page 1993](#)
- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1996](#)

### 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*.

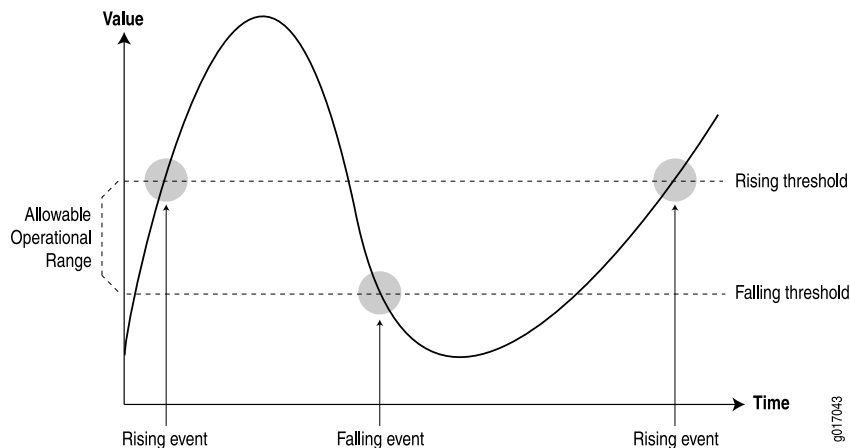
This topic includes the following sections:

- [Setting Thresholds on page 1993](#)
- [RMON Command-Line Interface on page 1994](#)
- [RMON Event Table on page 1994](#)
- [RMON Alarm Table on page 1995](#)
- [Troubleshooting RMON on page 1996](#)

#### 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 62 on page 1993](#).)

**Figure 62: Setting Thresholds**



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 277 on page 1995](#).) 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 277: RMON Event Table**

Field	Description
<b>eventDescription</b>	Text description of this event
<b>eventType</b>	Type of event (for example, <b>log</b> , <b>trap</b> , or <b>log and trap</b> )
<b>eventCommunity</b>	Trap group to which to send this event (as defined in the Junos OS configuration, which is not the same as the community)
<b>eventOwner</b>	Entity (for example, <b>manager</b> ) that created this event
<b>eventStatus</b>	Status of this row (for example, <b>valid</b> , <b>invalid</b> , or <b>createRequest</b> )

#### ***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 278 on page 1995](#).

**Table 278: RMON Alarm Table**

Field	Description
<b>alarmStatus</b>	Status of this row (for example, <b>valid</b> , <b>invalid</b> , or <b>createRequest</b> )
<b>alarmInterval</b>	Sampling period (in seconds) of the monitored variable
<b>alarmVariable</b>	OID (and instance) of the variable to be monitored
<b>alarmValue</b>	Actual value of the sampled variable
<b>alarmSampleType</b>	Sample type ( <b>absolute</b> or <b>delta</b> changes)
<b>alarmStartupAlarm</b>	Initial alarm ( <b>rising</b> , <b>falling</b> , or <b>either</b> )
<b>alarmRisingThreshold</b>	Rising threshold against which to compare the value
<b>alarmFallingThreshold</b>	Falling threshold against which to compare the value
<b>alarmRisingEventIndex</b>	Index (row) of the rising event in the event table
<b>alarmFallingEventIndex</b>	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 279 on page 1996](#) to the RFC 2819 **alarmTable**.

**Table 279: jnxRmon Alarm Extensions**

Field	Description
<b>jnxRmonAlarmGetFailCnt</b>	Number of times the internal <b>Get</b> request for the variable failed
<b>jnxRmonAlarmGetFailTime</b>	Value of <b>sysUpTime</b> when the last failure occurred
<b>jnxRmonAlarmGetFailReason</b>	Reason why the <b>Get</b> request failed
<b>jnxRmonAlarmGetOkTime</b>	Value of <b>sysUpTime</b> when the variable moved out of failure state
<b>jnxRmonAlarmState</b>	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 1996](#)

### 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 1996](#)
- [Basic Key Performance Indicators on page 1997](#)
- [Setting Baselines on page 1998](#)

#### Measurement Points

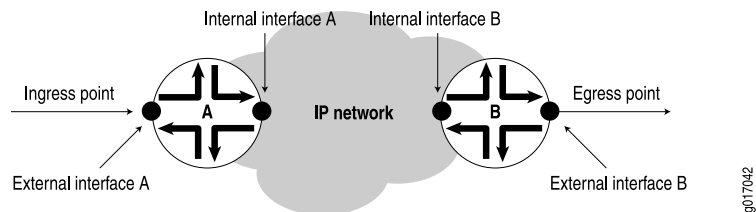
Defining the measurement points where metrics are measured is equally as important as defining the metrics themselves. This section describes measurement points within the context of this chapter and helps identify where measurements can be taken from

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 63 on page 1997](#).

- 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 63: Network Entry Points**



**NOTE:** [Figure 63 on page 1997](#) 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 1993](#)

---

## Health Monitoring with SNMP

- [Configuring Health Monitoring on page 1998](#)

### Configuring Health Monitoring

- [Configuring Health Monitoring on Devices Running Junos OS on page 1998](#)

---

#### 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 1999](#)
- [Minimum Health Monitoring Configuration on page 2000](#)
- [Configuring the Falling Threshold or Rising Threshold on page 2000](#)
- [Configuring the Interval on page 2000](#)
- [Log Entries and Traps on page 2001](#)

### **Monitored Objects**

When you configure the health monitor, monitoring information for certain object instances is available, as shown in [Table 280 on page 1999](#).

**Table 280: Monitored Object Instances**

Object	Description
<code>jnxHrStoragePercentUsed.1</code>	Monitors the following file system on the router or switch:  <code>/dev/ad0s1a:</code>  This is the root file system mounted on <code>/</code> .
<code>jnxHrStoragePercentUsed.2</code>	Monitors the following file system on the router or switch:  <code>/dev/ad0s1e:</code>  This is the configuration file system mounted on <code>/config</code> .
<code>jnxOperatingCPU (RE0)</code>	Monitors CPU usage for Routing Engines ( <b>RE0</b> and <b>RE1</b> ). 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 <b>RE1</b> is removed after five failed attempts to obtain the CPU value.
<code>jnxOperatingCPU (RE1)</code>	
<code>jnxOperatingBuffer (RE0)</code>	Monitors the amount of memory available on Routing Engines ( <b>RE0</b> and <b>RE1</b> ). 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 <b>RE1</b> is removed if the router or switch has only one Routing Engine.
<code>jnxOperatingBuffer (RE1)</code>	
<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.

Table 280: Monitored Object Instances (*continued*)

Object	Description
<code>sysApplElmtRunMemory</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 1986](#)
- [Configuring an Alarm Entry and Its Attributes on page 1987](#)
- [Configuring an Event Entry and Its Attributes on page 1991](#)
- [Example: Configuring Health Monitoring on page 1992](#)
- [Understanding Device Management Functions in Junos OS on page 1797](#)

---

## **Configuration Statements and Operational Commands**

- [Configuration Statements on page 2001](#)
- [Operational Commands on page 2089](#)

### **Configuration Statements**

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 2004](#)
- [Complete SNMPv3 Configuration Statements on page 2007](#)
- [access-list on page 2010](#)
- [address on page 2010](#)
- [address-mask on page 2011](#)
- [agent-address on page 2011](#)
- [alarm on page 2012](#)
- [authentication-md5 on page 2013](#)
- [authentication-none on page 2014](#)
- [authentication-password on page 2015](#)
- [authentication-sha on page 2016](#)
- [authorization on page 2017](#)
- [categories on page 2017](#)
- [client-list on page 2018](#)
- [client-list-name on page 2018](#)

- [clients on page 2019](#)
- [commit-delay on page 2019](#)
- [community on page 2020](#)
- [community on page 2021](#)
- [community-name on page 2022](#)
- [contact on page 2023](#)
- [description on page 2023](#)
- [description on page 2024](#)
- [destination-port on page 2024](#)
- [engine-id on page 2025](#)
- [enterprise-oid on page 2026](#)
- [event on page 2026](#)
- [falling-event-index on page 2027](#)
- [falling-threshold on page 2028](#)
- [falling-threshold on page 2029](#)
- [falling-threshold-interval on page 2030](#)
- [filter-duplicates on page 2030](#)
- [filter-interfaces on page 2031](#)
- [group \(Configuring Group Name\) on page 2032](#)
- [group \(Defining Access Privileges for an SNMPv3 Group\) on page 2033](#)
- [health-monitor on page 2033](#)
- [interface on page 2034](#)
- [interval on page 2034](#)
- [interval on page 2035](#)
- [local-engine on page 2036](#)
- [location on page 2037](#)
- [logical-system on page 2038](#)
- [logical-system-trap-filter on page 2039](#)
- [log-vital on page 2040](#)
- [message-processing-model on page 2042](#)
- [name on page 2042](#)
- [nonvolatile on page 2043](#)
- [notify on page 2044](#)
- [notify-filter \(Applying to the Management Target\) on page 2044](#)
- [notify-filter \(Configuring the Profile Name\) on page 2045](#)
- [notify-view on page 2045](#)
- [oid on page 2046](#)



- [oid on page 2046](#)
- [parameters on page 2047](#)
- [port on page 2047](#)
- [privacy-3des on page 2048](#)
- [privacy-aes128 on page 2049](#)
- [privacy-des on page 2050](#)
- [privacy-none on page 2050](#)
- [privacy-password on page 2051](#)
- [read-view on page 2052](#)
- [remote-engine on page 2053](#)
- [request-type on page 2054](#)
- [retry-count on page 2054](#)
- [rising-event-index on page 2055](#)
- [rising-threshold on page 2055](#)
- [rising-threshold on page 2056](#)
- [rmon on page 2056](#)
- [routing-engine \(SNMP Resource Level\) on page 2057](#)
- [routing-engine \(SNMP Global Level\) on page 2058](#)
- [routing-instance on page 2059](#)
- [routing-instance on page 2060](#)
- [routing-instance-access on page 2060](#)
- [sample-type on page 2061](#)
- [security-level \(Defining Access Privileges\) on page 2062](#)
- [security-level \(Generating SNMP Notifications\) on page 2063](#)
- [security-model \(Access Privileges\) on page 2064](#)
- [security-model \(Group\) on page 2065](#)
- [security-model \(SNMP Notifications\) on page 2065](#)
- [security-name \(Community String\) on page 2066](#)
- [security-name \(Security Group\) on page 2067](#)
- [security-name \(SNMP Notifications\) on page 2068](#)
- [security-to-group on page 2069](#)
- [snmp on page 2069](#)
- [source-address on page 2070](#)
- [snmp-community on page 2070](#)
- [startup-alarm on page 2071](#)
- [syslog-subtag on page 2071](#)
- [tag on page 2072](#)

- [tag-list](#) on page 2072
- [target-address](#) on page 2073
- [target-parameters](#) on page 2074
- [targets](#) on page 2075
- [timeout](#) on page 2075
- [traceoptions \(SNMP\)](#) on page 2076
- [trap-group](#) on page 2078
- [trap-options](#) on page 2079
- [type](#) on page 2079
- [type](#) on page 2080
- [user](#) on page 2080
- [usm](#) on page 2081
- [v3](#) on page 2083
- [vacm](#) on page 2085
- [variable](#) on page 2086
- [version](#) on page 2086
- [view \(Associating a MIB View with a Community\)](#) on page 2087
- [view \(Configuring a MIB View\)](#) on page 2088
- [write-view](#) on page 2089

### **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 {
 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;
}
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 on page 1800](#)
- [Configuring SNMP on a Device Running Junos OS on page 1898](#)

#### 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 1917](#)
- [Configuring MIB Views on page 1906](#)
- [Defining Access Privileges for an SNMP Group on page 1926](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1936](#)
- [Configuring SNMP Informs on page 1935](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1922](#)

## 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. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">routing-instance-access on page 2060</a></li></ul>

## address

---

<b>Syntax</b>	<pre>address <i>address</i>;</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. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Specify the SNMP target address.
<b>Options</b>	<b>address</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. 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 on page 1939</a></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. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Verify the source addresses for a group of target addresses.
<b>Options</b>	<b><i>address-mask</i></b> combined with the address defines a range of addresses.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1940</a></li> </ul>

## agent-address

---

<b>Syntax</b>	<code>agent-address outgoing-interface;</code>
<b>Hierarchy Level</b>	<code>[edit snmp trap-options]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. <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. 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 1911</a></li> </ul>

## alarm

---

<b>Syntax</b>	<pre>alarm <i>index</i> {     <i>description</i> <i>description</i>;     <i>falling-event-index</i> <i>index</i>;     <i>falling-threshold</i> <i>integer</i>;     <i>falling-threshold-interval</i> <i>seconds</i>;     <i>interval</i> <i>seconds</i>;     <i>request-type</i> (get-next-request   get-request   walk-request);     <i>rising-event-index</i> <i>index</i>;     <i>rising-threshold</i> <i>integer</i>;     <i>sample-type</i> (absolute-value   delta-value);     <i>startup-alarm</i> (falling-alarm   rising-alarm   rising-or-falling alarm);     <i>syslog-subtag</i> <i>syslog-subtag</i>;     <i>variable</i> <i>oid-variable</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp rmon]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure RMON alarm entries.
<b>Options</b>	<i>index</i> —Identifies this alarm entry as an integer.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1987</a></li><li>• <a href="#">event on page 2026</a></li></ul>

## authentication-md5

---

<b>Syntax</b>	authentication-md5 { authentication-password <i>authentication-password</i> ; }
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ], [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. 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 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. 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 1924</a></li> </ul>

## authentication-none

---

<b>Syntax</b>	authentication-none;
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ], [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. 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 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. 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 1924</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], [edit snmp v3 usm local-engine user <i>username</i> authentication-sha], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> authentication-md5], [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. 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 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. 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 1924</a></li><li>• <a href="#">Configuring SHA Authentication on page 1924</a></li></ul>

## authentication-sha

---

<b>Syntax</b>	<code>authentication-sha {     <code>authentication-password</code> <i>authentication-password</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ], [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. 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 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. 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 1924</a></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. 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>	Set the access authorization for SNMP <b>Get</b> , <b>GetBulk</b> , <b>GetNext</b> , and <b>Set</b> requests.
<b>Options</b>	<p><b><i>authorization</i></b>—Access authorization level:</p> <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> <p><b>Default:</b> read-only</p>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring the SNMP Community String on page 1902</a></li> </ul>

## categories

<b>Syntax</b>	<pre>categories {   category; }</pre>
<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. 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>	<b><i>category</i></b> —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>sonet-alarms</b> , <b>startup</b> , or <b>vrp-events</b> .
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1912</a></li> </ul>

## client-list

---

<b>Syntax</b>	<code>client-list <i>client-list-name</i> {     <i>ip-addresses</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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.  <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. 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 1944</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. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for FX 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. 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 1944</a></li></ul>



## clients

---

<b>Syntax</b>	<pre>clients {     address &lt;restrict&gt;; }</pre>
<b>Hierarchy Level</b>	[edit snmp community <i>community-name</i> ]
<b>Release Information</b>	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 FX 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.  <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. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the SNMP Community String on page 1902</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. 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. <b>Default:</b> 5 seconds
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1902</a></li></ul>

## community

---

<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>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<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><i>community-name</i></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 the SNMP Community String on page 1902</a></li></ul>


## community

---

<b>Syntax</b>	<code>community <i>community-name</i>;</code>
<b>Hierarchy Level</b>	[edit snmp rmon event <i>index</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	snmp—To view this statement in the configuration. 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 1991</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. 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 (" ").
<hr/>	
<div> <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.</div> <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><hr/></div>	
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 SNMPv3 Community on page 1945</a></li></ul>

## contact

---

<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. 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. 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 1900</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. 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>	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. 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 1901</a></li> </ul>

## description

---


<b>Syntax</b>	<code>description <i>description</i>;</code>
<b>Hierarchy Level</b>	[edit snmp rmon alarm <i>index</i> ], [edit snmp rmon event <i>index</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Text description of alarm or event.
<b>Options</b>	<i>description</i> —Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—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 1988</a></li><li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1991</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. 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. 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 1912</a></li></ul>

## engine-id

<b>Syntax</b>	engine-id { (local <i>engine-id-suffix</i>   use-default-ip-address   use-mac-address); }
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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 1934</a></li> </ul>

## enterprise-oid

---

<b>Syntax</b>	enterprise-oid;
<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. 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 1909</a></li></ul>

## event

---

<b>Syntax</b>	event <i>index</i> { <a href="#">community</a> <i>community-name</i> ; <a href="#">description</a> <i>description</i> ; <a href="#">type</a> <i>type</i> ; }
<b>Hierarchy Level</b>	[edit snmp <a href="#">rmon</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure RMON event entries.
<b>Options</b>	<i>index</i> —Identifier for a specific event entry.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1991</a></li><li>• <a href="#">alarm on page 2012</a></li></ul>



## falling-event-index

---

<b>Syntax</b>	<code>falling-event-index <i>index</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. 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>	<i>index</i> —Index of the event entry that is used when a falling threshold is crossed. <b>Range:</b> 0 through 65,535 <b>Default:</b> 0
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1988</a></li><li>• <a href="#">rising-event-index on page 2055</a></li></ul>

## 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. 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. <b>Range:</b> 1 through 100 <b>Default:</b> 70 percent of the maximum possible value
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 2000</a></li><li>• <a href="#">rising-threshold on page 2056</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. 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. <b>Range:</b> -2,147,483,648 through 2,147,483,647 <b>Default:</b> 20 percent less than <b>rising-threshold</b>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1988</a></li><li>• <a href="#">rising-threshold on page 2055</a></li></ul>

## falling-threshold-interval

---

<b>Syntax</b>	<code>falling-threshold-interval seconds;</code>
<b>Hierarchy Level</b>	<code>[edit snmp rmon <a href="#">alarm index</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. 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. <b>Range:</b> 1 through 2,147,483,647 seconds <b>Default:</b> 60 seconds
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Falling Threshold Interval on page 1989</a></li><li>• <a href="#">interval on page 2034</a></li></ul>

## filter-duplicates

---

<b>Syntax</b>	<code>filter-duplicates;</code>
<b>Hierarchy Level</b>	<code>[edit snmp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —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 1904</a></li></ul>

## filter-interfaces

---

<b>Syntax</b>	<pre>filter-interfaces {   interfaces {     all-internal-interfaces;     interface 1;     interface 2;   } }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4. 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>	<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="#">Filtering Interface Information Out of SNMP Get and GetNext Output on page 1905</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.

**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. 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.

The remaining statements under this hierarchy are documented in separate topics.

**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 1928](#)

## 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) security-name security-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<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. 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 1933</a></li></ul>

## health-monitor

---

<b>Syntax</b>	<pre>health-monitor {   falling-threshold percentage;   interval seconds;   rising-threshold percentage; }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure health monitoring.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1998</a></li></ul>

## interface

---

<b>Syntax</b>	<code>interface [ <i>interface-names</i> ];</code>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	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 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>	snmp—To view this statement in the configuration. snmp-control—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 1905</a></li></ul>

## interval

---

<b>Syntax</b>	<code>interval <i>seconds</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. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Interval between samples.
<b>Options</b>	<i>seconds</i> —Time between samples, in seconds. <b>Range:</b> 1 through 2,147,483,647 seconds <b>Default:</b> 60 seconds
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1989</a></li></ul>



## interval

---

<b>Syntax</b>	<code>interval seconds;</code>
<b>Hierarchy Level</b>	[edit snmp health-monitor]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0. 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. <b>Range:</b> 1 through 2147483647 seconds <b>Default:</b> 300 seconds
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 2000</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 1917](#)

## location

---

<b>Syntax</b>	<code>location <i>location</i>;</code>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	snmp—To view this statement in the configuration. 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 Location for a Device Running Junos OS on page 1900</a></li></ul>

## logical-system

<b>Syntax</b>	<code>logical-system <i>logical-system-name</i> {     <i>routing-instance routing-instance-name</i>; }</code>
<b>Hierarchy Level</b>	<code>[edit snmp <i>community community-name</i>], [edit snmp <i>trap-group</i>], [edit snmp <i>trap-options</i>] [edit snmp <i>v3target-address target-address-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3 Statement introduced in Junos OS Release 9.0 for EX Series switches.
<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 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 1956</a></li> <li>• <a href="#">Configuring the Trap Target Address on page 1939</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. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Trap Support for Routing Instances on page 1954</a></li></ul>

## log-vital

<b>Syntax</b>	<pre> log-vital {   add &lt;oid&gt; {     comment &lt;comment&gt;;   }   file-size;   files;   group {     operating;     idp;     storage;     cluster-counter;     screen;     spu;   }   interval;   storage-limit; } </pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X47-D15.
<b>Description</b>	Configure vital log data.
<b>Options</b>	<p><b>add&lt;oid&gt;</b>—Specify the OID to be used to collect the raw data.</p> <ul style="list-style-type: none"> <li><b>comment</b>—Specify the comment for the raw OID.</li> </ul> <p><b>file-size</b>—Specify the size of the current dump file.</p> <p><b>Range:</b> 1 MB to 100 MB.</p> <p><b>Default:</b> 5 MB for branch SRX Series devices and 10 MB for high-end SRX Series devices.</p> <p><b>files</b>—Specify the lifetime (number of days) for the dump file to be stored. The dump file is stored at <code>/var/log/vital/</code>.</p> <p><b>Range:</b> 1 to 30 days.</p> <p><b>Default:</b> 3 days.</p> <p><b>group</b>—Specify the pre-defined OID group to be used. Each group contains multiple OIDs within the same area. Once a group enabled, all OIDs in the group will be periodically collected and dumped.</p> <ul style="list-style-type: none"> <li><b>operating</b>—This group includes state, temperature, current CPU utilization percentage, buffer utilization percentage, heap-utilization percentage, up time, average-load in the last 1 minute, 5 minutes, or 15 minutes, and buffer-pool utilization percentage in the control plane of each operating component in the system.</li> <li><b>idp</b>—This group includes IDP data plane memory usage, IDP session usage and policies loaded number.</li> </ul>

- **storage**—This group includes storage utilization of directory `/var/log`.
- **cluster-counter**—This group includes current total session number, total CPS, IPv4 CPS, IPv6 CPS, current total IPv4 session number, and current total IPv6 session number of both node 0 and node 1.
- **screen**—This group includes screen statistics of a specified zone.
- **spu**—This group includes CPU usage, memory usage, current flow session number, current CP session number, IPv4 session number, IPv6 session number, CP IPv4 session number, and CP IPv6 session number of the SPU.

**interval**—Specify the collection interval in minutes. The configuration takes effect immediately with new interval value.

**Range:** 1 to 1440 minutes.

**Default:** 10 minutes.

**storage-limit**—Specify the storage usage limit in percentage. If the current storage usage of the directory `/var/log/` is above the upper limit, collection is canceled but is tried next time.

**Range:** 1 to 100 percent.

**Default:** 80 percent.

<b>Required Privilege Level</b>	security—To view this statement in the configuration.
	security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show system log-vital on page 2105</a></li></ul>

## message-processing-model

---

<b>Syntax</b>	<code>message-processing-model (v1   v2c   v3);</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 target-parameters <i>target-parameter-name</i> parameters]</code>
<b>Release Information</b>	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 the message processing model to be used when generating SNMP notifications.
<b>Options</b>	<code>v1</code> —SNMPv1 message process model.  <code>v2c</code> —SNMPv2c message process model.  <code>v3</code> —SNMPv3 message process model.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Message Processing Model on page 1942</a></li></ul>

## name

---

<b>Syntax</b>	<code>name <i>name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	<code>name</code> —System name override.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Name on page 1901</a></li></ul>



## nonvolatile

---

<b>Syntax</b>	<code>nonvolatile {     <a href="#">commit-delay</a> <i>seconds</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. The <a href="#">commit-delay</a> statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure options for SNMP <b>Set</b> requests.  The statement is explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1902</a></li><li>• <a href="#">commit-delay on page 2019</a></li></ul>

## notify

---

<b>Syntax</b>	<code>notify <i>name</i> {     tag <i>tag-name</i>;     type (trap   inform); }</code>
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>type inform</b> option added in 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>	Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.
<b>Options</b>	<b><i>name</i></b> —Name assigned to the notification.  <b><i>tag-name</i></b> —Notifications are sent to all targets configured with this tag.  <b><i>type</i></b> —Notification type is <b>trap</b> or <b>inform</b> . Traps are unconfirmed notifications. Informs are confirmed notifications.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Inform Notification Type and Target Address on page 1948</a></li><li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1937</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>	[edit snmp v3 <b>target-parameters</b> <i>target-parameters-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Specify the notify filter to be used by a specific set of target parameters.
<b>Options</b>	<b><i>profile-name</i></b> —Name of the notify filter to apply to notifications.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1942</a></li></ul>

## notify-filter (Configuring the Profile Name)

<b>Syntax</b>	<code>notify-filter <i>profile-name</i> {     oid <i>oid</i> (include   exclude); }</code>
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Release Information</b>	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>	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.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1915</a></li> <li>• <a href="#">oid on page 2046</a></li> </ul>

## notify-view

<b>Syntax</b>	<code>notify-view <i>view-name</i>;</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. 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>	Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).
<b>Options</b>	<i>view-name</i> —Name of the view to which the SNMP user group has access.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1906</a></li> <li>• <a href="#">Configuring the Notify View on page 1930</a></li> </ul>

## oid

---

<b>Syntax</b>	<code>oid <i>object-identifier</i> (exclude   include);</code>
<b>Hierarchy Level</b>	<code>[edit snmp view <i>view-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. <b>include</b> —Include the subtree of MIB objects represented by the specified OID. <b><i>object-identifier</i></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>	<code>snmp</code> —To view this statement in the configuration. <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 MIB Views on page 1906</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. 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. <b>include</b> —Include the subtree of MIB objects represented by the specified OID. <b><i>oid</i></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>	<code>snmp</code> —To view this statement in the configuration. <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 Trap Notification Filter on page 1915</a></li></ul>

## parameters

---

<b>Syntax</b>	<pre>parameters {   message-processing-model (v1   v2c   v3);   security-level (none   authentication   privacy);   security-model (usm   v1   v2c);   security-name security-name; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> ]
<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 a set of target parameters for message processing and 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="#">Defining and Configuring the Trap Target Parameters on page 1941</a></li> </ul>

## port

---

<b>Syntax</b>	<code>port port-number;</code>
<b>Hierarchy Level</b>	[edit snmp v3 target-address <i>target-address-name</i> ]
<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>	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>	<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 Port on page 1940</a></li> </ul>

## privacy-3des

---

<b>Syntax</b>	<pre>privacy-3des {     <b>privacy-password</b> <i>privacy-password</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ], [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. 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 the triple Data Encryption Standard (3DES) 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. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Encryption Type on page 1925</a></li></ul>

## privacy-aes128

---

<b>Syntax</b>	<pre>privacy-aes128 {   <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 Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) 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 Encryption Type on page 1925</a></li> </ul>

## privacy-des

---

<b>Syntax</b>	<code>privacy-des {     privacy-password <i>privacy-password</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ], [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. 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 the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.
<b>Options</b>	<code>privacy-password <i>privacy-password</i></code> —Password that a user enters. The password is then converted into a key that is used for encryption.  SNMPv3 has special requirements when you create plain-text passwords on a router or switch: <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. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Encryption Type on page 1925</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> ], [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. 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 that no encryption be used for the SNMPv3 user.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Encryption Type on page 1925</a></li></ul>



## privacy-password

<b>Syntax</b>	<code>privacy-password <i>privacy-password</i>;</code>
<b>Hierarchy Level</b>	<p>[edit snmp v3 usm local-engine user <i>username</i> privacy-3des],          [edit snmp v3 usm local-engine user <i>username</i> privacy-aes128],          [edit snmp v3 usm local-engine user <i>username</i> privacy-des],          [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-3des],          [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-aes128],          [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-des]</p>
<b>Release Information</b>	<p>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.</p>
<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>	<p>snmp—To view this statement in the configuration.          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 Encryption Type on page 1925</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. 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>	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. <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 1930</a></li><li>• <a href="#">Configuring MIB Views on page 1906</a></li></ul>

## remote-engine

```
Syntax 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 usm]

**Release Information** Statement introduced in 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 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.

**Options** *engine-id*—Engine identifier. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

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 the Remote Engine and Remote User on page 1950](#)

## request-type

---

<b>Syntax</b>	<code>request-type (get-next-request   get-request   walk-request);</code>
<b>Hierarchy Level</b>	<code>[edit snmp rmon <a href="#">alarm index</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. 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.  <b>get-request</b> —Performs an SNMP get request.  <b>walk-request</b> —Performs an SNMP walk request. <b>Default:</b> <code>walk-request</code>
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Request Type on page 1989</a></li><li>• <a href="#">variable on page 2086</a></li></ul>

## retry-count

---

<b>Syntax</b>	<code>retry-count <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 <a href="#">target-address target-address-name</a>]</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>	<b><i>number</i></b> —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. <b>Default:</b> 3 times
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 1935</a></li><li>• <a href="#">timeout on page 2075</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. 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. <b>Range:</b> 0 through 65,535 <b>Default:</b> 0
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Falling Event Index or Rising Event Index on page 1988</a></li> <li>• <a href="#">falling-event-index on page 2027</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. 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. <b>Range:</b> -2,147,483,648 through 2,147,483,647
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 Falling Threshold or Rising Threshold on page 1988</a></li> <li>• <a href="#">falling-threshold on page 2029</a></li> </ul>

## rising-threshold

---

<b>Syntax</b>	<code>rising-threshold <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp ]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0. 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. <b>Range:</b> 1 through 100 <b>Default:</b> 80 percent of the maximum possible value
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 2028</a></li><li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 2000</a></li></ul>

## rmon

---

<b>Syntax</b>	<code>rmon { ... }</code>
<b>Hierarchy Level</b>	<code>[edit snmp]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. 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 1987</a></li></ul>

## routing-engine (SNMP Resource Level)

**Syntax**    routing-engine {  
               resource <cpu | memory | open-files-count | process-count | storage | temperature> ;  
               {  
                   interval <interval in secs>;  
                   moderate-threshold <percentage level>;  
                   high-threshold <percentage level>;  
                   critical-threshold <percentage level>;  
                   action <monitor | prevent | recover>;  
               }  
           }

**Hierarchy Level**    [edit snmp health-monitor routing-engine]

**Release Information**    Statement introduced in Junos OS Release 12.1X44-D10. Statement modified in Junos OS Release 12.1X45-D10.

**Description**    Override the global configuration for a resource.

- Options**
- **interval**—Monitoring interval in seconds.  
       Default: 300 seconds
  - **moderate-threshold**—Percentage of moderate threshold level resource utilization.  
       Default: 70 percent.
  - **high-threshold** —Percentage of high-threshold level resource utilization.  
       Default: 80 percent.
  - **critical-threshold** —Percentage of critical threshold level resource utilization.  
       Default: 90 percent.
  - **action**—Enable action for all resources.  
       Default: If action is not enabled, the default action is prevent.



**WARNING:** If the system health management action for an affected resource is configured to recover, then certain intrusive operations necessary for preventing system breakdown are taken. Intrusive operations can include restarting or terminating processes, deleting files, and so on. Such action information is logged in the system health management history and system log.

**Required Privilege Level**    security—To view this statement in the configuration.  
                                   security-control—To add this statement to the configuration.

## routing-engine (SNMP Global Level)

**Syntax**    routing-engine

```
{
 interval <interval in secs>;
 moderate-threshold <percentage level>;
 high-threshold <percentage level>;
 critical-threshold <percentage level>;
 traceoptions;
 action <monitor | prevent | recover>;
}
```

**Hierarchy Level**    [edit snmp health-monitor routing-engine]

**Release Information**    Statement introduced in Junos OS Release 12.1X44-D10. Statement modified in Junos OS Release 12.1X45-D10.

**Description**    Enable the system health management feature to use the specified parameters.

- Options**
- **interval**—Monitoring interval in seconds.  
Default: 300 seconds
  - **moderate-threshold**—Percentage of moderate threshold level resource utilization.  
Default: 70 percent.
  - **high-threshold** —Percentage of high-threshold level resource utilization.  
Default: 80 percent.
  - **critical-threshold** —Percentage of critical threshold level resource utilization.  
Default: 90 percent.
  - **traceoptions**—Enable tracing of system health monitoring daemon.
  - **action**—Enable action for all resources.  
Default: If action is not enabled, the default is prevent.



**WARNING:** If the system health management action for an affected resource is configured to recover, then certain intrusive operations necessary for preventing system breakdown are taken. Intrusive operations can include restarting or terminating processes, deleting files, and so on. Such action information is logged in the system health management history and system log.

**Required Privilege Level**

security	—To view this statement in the configuration.
security-control	—To add this statement to the configuration.



## routing-instance

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp <b>community</b> <i>community-name</i>],</code> <code>[edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical-system-name</i>],</code> <code>[edit snmp <b>trap-group</b> <i>group</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. Added to the <code>[edit snmp <b>community</b> <i>community-name</i>]</code> hierarchy level in Junos OS Release 8.4. Added to the <code>[edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical-system-name</i>]</code> hierarchy level in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Specify a routing instance for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use this routing instance.  If the routing instance is defined within a logical system, include the <b>logical-system <i>logical-system-name</i></b> statement at the <code>[edit snmp <b>community</b> <i>community-name</i>]</code> hierarchy level and specify the <b>routing-instance</b> statement under the <code>[edit snmp <b>community</b> <i>community-name</i> logical-system <i>logical-system-name</i>]</code> hierarchy level.
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance.
<b>Required Privilege Level</b>	<b>snmp</b> —To view this statement in the configuration. <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 1912</a></li> <li>• <a href="#">Configuring the Source Address for SNMP Traps on page 1909</a></li> <li>• <a href="#">Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1956</a></li> </ul>

## routing-instance

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 <a href="#">target-address</a> <i>target-address-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. 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>	<code>snmp</code> —To view this statement in the configuration. <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 Trap Target Address on page 1939</a></li></ul>

## routing-instance-access

---

<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>	<code>[edit snmp]</code>
<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>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —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 1956</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. 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. 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 1990</a></li></ul>

## security-level (Defining Access Privileges)

---

<b>Syntax</b>	<pre>security-level (authentication   none   privacy) {     notify-view view-name;     read-view view-name;     write-view view-name; }</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. 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>	Define the security level used for access privileges.
<b>Default</b>	none
<b>Options</b>	<b>authentication</b> —Provide authentication but no encryption.  <b>none</b> —No authentication and no encryption.  <b>privacy</b> —Provide authentication and encryption.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1928</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. 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 the security level to use when generating SNMP notifications.
<b>Default</b>	none
<b>Options</b>	<b>authentication</b> —Provide authentication but no encryption.  <b>none</b> —No authentication and no encryption.  <b>privacy</b> —Provide authentication and encryption.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1943</a></li></ul>

## security-model (Access Privileges)

---

<b>Syntax</b>	security-model (usm   v1   v2c);
<b>Hierarchy Level</b>	[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i> )]
<b>Release Information</b>	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 the security model for an SNMPv3 group. The security model is used to determine access privileges for the group.
<b>Options</b>	<b>usm</b> —SNMPv3 security model.  <b>v1</b> —SNMPv1 security model.  <b>v2c</b> —SNMPv2c security model.
<b>Required Privilege Level</b>	<b>snmp</b> —To view this statement in the configuration. <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 1928</a></li></ul>

## security-model (Group)


<b>Syntax</b>	security-model (usm   v1   v2c) { security-name security-name { group group-name; } }
<b>Hierarchy Level</b>	[edit snmp v3 vacm security-to-group]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	usm—SNMPv3 security model.  v1—SNMPv1 security model.  v2c—SNMPv2c security model.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 Model on page 1932</a></li> </ul>

## security-model (SNMP Notifications)

<b>Syntax</b>	security-model (usm   v1   v2c);
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters target-parameters-name parameters]
<b>Release Information</b>	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 the security model for an SNMPv3 group. The security model is used for SNMP notifications.
<b>Options</b>	usm—SNMPv3 security model.  v1—SNMPv1 security model.  v2c—SNMPv2c security model.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 Model on page 1943</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. 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>	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. <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 1947</a></li></ul>




## security-name (Security Group)

---

<b>Syntax</b>	<code>security-name <i>security-name</i> {     <i>group</i> <i>group-name</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp v3 vacm security-to-group <i>security-model</i> (usm   v1   v2c)]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	<i>security-name</i> —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. 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 1932</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. 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 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.
<div>  <p><b>NOTE:</b> The access privileges for the group associated with this security name must allow this notification to be sent.</p> <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> </div>	
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 Name on page 1943</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 1932</a></li> </ul>

## snmp

---

<b>Syntax</b>	snmp { ... }
<b>Hierarchy Level</b>	[edit]
<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 SNMP.
<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 on a Device Running Junos OS on page 1898</a></li> </ul>

## source-address

---

<b>Syntax</b>	source-address <i>address</i> ;
<b>Hierarchy Level</b>	[edit snmp trap-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>address</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> . <b>Default:</b> Disabled. (The source address is the address of the outgoing interface.)
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—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 1909</a></li></ul>

## snmp-community

---

<b>Syntax</b>	snmp-community <i>community-index</i> { <b>community-name</b> <i>community-name</i> ; <b>security-name</b> <i>security-name</i> ; <b>tag</b> <i>tag-name</i> ; }
<b>Hierarchy Level</b>	[edit snmp <b>v3</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the SNMP community.
<b>Options</b>	<b>community-index</b> —(Optional) String that identifies an SNMP community.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1945</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</a> index]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. 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 1990</a></li> </ul>

## syslog-subtag

---

<b>Syntax</b>	syslog-subtag <i>syslog-subtag</i> ;
<b>Hierarchy Level</b>	[edit snmp rmon <a href="#">alarm</a> index]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. 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. 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 1990</a></li> </ul>

## tag

---

<b>Syntax</b>	<code>tag tag-name;</code>
<b>Hierarchy Level</b>	[edit snmp v3 <a href="#">notify name</a> ], [edit snmp v3 <a href="#">snmp-community community-index</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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. 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 1947</a></li><li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1937</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. 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 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. 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 1940</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>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<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>	snmp—To view this statement in the configuration. 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 1939</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 1941](#)
- [Applying Target Parameters on page 1941](#)



## targets

---

<b>Syntax</b>	<code>targets {     <i>address</i>; }</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. 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>	<code>snmp</code> —To view this statement in the configuration. <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 1912</a></li> </ul>

## timeout

---

<b>Syntax</b>	<code>timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 <a href="#">target-address</a> <i>target-address-name</i>]</code>
<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. <b>Default:</b> 15
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 1935</a></li> <li>• <a href="#">retry-count on page 2054</a></li> </ul>

## traceoptions (SNMP)

<b>Syntax</b>	<pre> traceoptions {     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>traceoptions</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>	<b>snmp</b> —To view this statement in the configuration. <b>snmp-control</b> —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 1969</a></li></ul>
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------

## trap-group

---

<b>Syntax</b>	<pre>trap-group <i>group-name</i> {     <b>categories</b> {         <i>category</i>;     }     <b>destination-port</b> <i>port-number</i>;     <b>routing-instance</b> <i>instance</i>;     <b>targets</b> {         <i>address</i>;     }     <b>version</b> (all   v1   v2); }</pre>
<b>Hierarchy Level</b>	[edit snmp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<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>	snmp—To view this statement in the configuration. 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 1912</a></li></ul>

## trap-options

<b>Syntax</b>	<pre>trap-options {     agent-address outgoing-interface;     source-address address; }</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>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>	<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 Options on page 1909</a></li> </ul>

## type

<b>Syntax</b>	type (inform   trap);
<b>Hierarchy Level</b>	[edit snmp v3 notify <i>name</i> ]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>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>
<b>Description</b>	Configure the type of SNMP notification.
<b>Options</b>	<p><b>inform</b>—Defines the type of notification as an inform. SNMP informs are confirmed notifications.</p> <p><b>trap</b>—Defines the type of notification as a trap. SNMP traps are unconfirmed 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 SNMP Informs on page 1935</a></li> <li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1937</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. 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>	<b>type</b> —Type of notification: <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> <b>Default:</b> log-and-trap
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1991</a></li></ul>

## user

---

<b>Syntax</b>	<code>user username;</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine], [edit snmp v3 usm remote-engine <i>engine-id</i> ]
<b>Release Information</b>	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>	Specify a user associated with an SNMPv3 group on a local or remote SNMP engine.
<b>Options</b>	<b>username</b> —SNMPv3 user-based security model (USM) username.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1917</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.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1917</a></li><li>• <a href="#">Configuring the Remote Engine and Remote User on page 1950</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.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1922</a></li> </ul>

## vacm

<b>Syntax</b>	<pre>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;     }   } }</pre>
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure view-based access control model (VACM) information.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1926</a></li> </ul>

## variable

---

<b>Syntax</b>	<code>variable <i>oid-variable</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. 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>	<i>oid-variable</i> —OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, 1.3.6.1.2.1.2.1.2.1.10.1). Alternatively, use the MIB object name (for example, <code>ifInOctets.1</code> ).
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1991</a></li></ul>

## version

---

<b>Syntax</b>	<code>version (all   v1   v2);</code>
<b>Hierarchy Level</b>	[edit snmp trap-group <i>group-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	all—Send an SNMPv1 and SNMPv2 trap for every trap condition.
<b>Options</b>	all—Send an SNMPv1 and SNMPv2 trap for every trap condition.  v1—Send SNMPv1 traps only.  v2—Send SNMPv2 traps only.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1912</a></li></ul>


## view (Associating a MIB View with a Community)

---

<b>Syntax</b>	<code>view view-name;</code>
<b>Hierarchy Level</b>	<code>[edit snmp community community-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>view-name</b> —Name of the view. You must use a view name already configured in the <b>view</b> statement at the <code>[edit snmp]</code> hierarchy level.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <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 SNMP Community String on page 1902</a></li></ul>

## view (Configuring a MIB View)

---

Syntax	<pre>view view-name {     oid object-identifier (include   exclude); }</pre>
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.
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 [edit snmp community <i>community-name</i> ] 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>view-name</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 1906</a></li><li>• <a href="#">Associating MIB Views with an SNMP User Group on page 1929</a></li><li>• <a href="#">community on page 2020</a></li></ul>

## write-view

---

<b>Syntax</b>	<code>write-view <i>view-name</i>;</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. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series switches.
<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>	<i>view-name</i> —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. 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 1906</a></li> <li>• <a href="#">Configuring the Write View on page 1930</a></li> </ul>

## Operational Commands

- `show snmp health-monitor`
- `show snmp health-monitor routing-engine history`
- `show snmp health-monitor routing-engine status`
- `show snmp mib (View)`
- `show system log-vital`

## show snmp health-monitor

<b>Syntax</b>	show snmp health-monitor <alarms <detail>>   <logs>
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D10 for SRX Series devices.
<b>Description</b>	Display information about SNMP health monitor alarms and logs.
<b>Options</b>	<b>none</b> —Display information about all health monitor alarms and logs. <b>alarms &lt;detail&gt;</b> —(Optional) Display detailed information about health monitor alarms. <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 2092</a> <a href="#">show snmp health-monitor alarms detail on page 2093</a> <a href="#">show snmp health-monitor alarms brief on page 2094</a>
<b>Output Fields</b>	<a href="#">Table 281 on page 2090</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 281: show snmp health-monitor Output Fields

Field Name	Field Description
Alarm Index	Alarm identifier.
Variable description	Description of the health monitor object instance being monitored.
Variable name	Name of the health monitor object instance being monitored.
Value	Current value of the monitored variable in the most recent sample interval.



Table 281: show snmp health-monitor Output Fields (*continued*)

Field Name	Field Description
<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>moderate-threshold</b>—Percentage of moderate threshold level resource utilization.</li> <li><b>high-threshold</b>—Percentage of high-threshold level resource utilization.</li> <li><b>critical-threshold</b>—Percentage of critical threshold level resource utilization.</li> <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>
<b>Variable OID</b>	Object ID to which the variable name is resolved. The format is x.x.x.x.
<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>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>
<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>Creator</b>	Mechanism by which the entry was configured ( <b>Health Monitor</b> ).

Table 281: show snmp health-monitor Output Fields (*continued*)

Field Name	Field Description
Sample interval	Time period between samples (in seconds).
Rising threshold	Upper limit threshold value as a percentage of the maximum possible value.
Falling threshold	Lower limit threshold value as a percentage of the maximum possible value.
Rising event index	Event triggered when the rising threshold is crossed.
Falling event index	Event triggered when the falling threshold is crossed.

## Sample Output

### show snmp health-monitor

```
user@host> show snmp health-monitor
```

Alarm Index	Variable description	Value	State
32770	Health Monitor: md3:/jail/mfs utilization jnxHrStoragePercentUsed.16	0	active
32773	Health Monitor: md2:/mfs/var/run/utm utilization jnxHrStoragePercentUsed.15	0	active
32776	Health Monitor: md1:/mfs utilization jnxHrStoragePercentUsed.11	11	active
32779	Health Monitor: /var file system utilization jnxHrStoragePercentUsed.10	44	critical threshold
32782	Health Monitor: root file system utilization jnxHrStoragePercentUsed.1	52	critical threshold
32785	Health Monitor: /config file system utilization jnxHrStoragePercentUsed.2	0	active
32788	Health Monitor: RE 0 CPU utilization jnxOperatingCPU.9.1.0.0	20	active
32791	Health Monitor: RE 0 memory utilization jnxOperatingBuffer.9.1.0.0	52	active
32792	Health Monitor: Max Kernel Memory Used (%) jnxBoxKernelMemoryUsedPercent.0	3	active
32793	Health Monitor: jroute daemon memory usage		
	Routing protocols process	51452	active
	Management process	38284	active
	Periodic packet management process	9828	active
	Bidirectional Forwarding Detection process	13088	active
	Service Deployment Client	10012	active
	Event processing process	12692	active
	Layer 2 address flooding and learning process	20212	active

MPLS Periodic Traceroute process	10488 active
Multicast Snooping process	9608 active
Feature license management process	12372 active

## show snmp health-monitor alarms detail

user@host> show snmp health-monitor alarms detail

```

Alarm Index 32770:
Variable name jnxHrStoragePercentUsed.16
Variable OID 1.3.6.1.4.1.2636.3.31.1.1.1.1.16
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: md3:/jail/mfs utilization

```

```

Creator Health Monitor
State active
Sample interval 15 seconds
Moderate threshold 20
High threshold 30
Critical threshold 40
Rising event index 32768
Falling event index 32768
Instance Value: 0
Instance State: active

```

```

Alarm Index 32773:
Variable name jnxHrStoragePercentUsed.15
Variable OID 1.3.6.1.4.1.2636.3.31.1.1.1.1.15
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: md2:/mfs/var/run/utm
 utilization
Creator Health Monitor
State active
Sample interval 15 seconds
Moderate threshold 20
High threshold 30
Critical threshold 40
Rising event index 32768
Falling event index 32768
Instance Value: 0
Instance State: active

```

```

Alarm Index 32793:
Variable name sysAppElmtRunMemory.5
Variable OID 1.3.6.1.2.1.54.1.2.3.1.10.5
Sample type absolute value
Startup alarm rising alarm
Owner Health Monitor: jroute daemon memory
 usage
Creator Health Monitor
State active
Sample interval 20 seconds
Rising threshold 104857
Falling threshold 91750
Rising event index 32768
Falling event index 32768
Instance Name: sysAppElmtRunMemory.5.5.1258
Instance Description: Routing protocols process

```

Instance Value: 51452  
Instance State: active

Instance Name: sysAppElemRunMemory.5.6.1255  
Instance Description: Management process  
Instance Value: 38284  
Instance State: active

Instance Name: sysAppElemRunMemory.5.6.3816  
Instance Description: Management process  
Instance Value: 38352  
Instance State: active

Instance Name: sysAppElemRunMemory.5.8.3815  
Instance Description: Command-line interface  
Instance Value: 49108  
Instance State: active

### show snmp health-monitor alarms brief

```

user@host> show snmp health-monitor alarms brief
32791 Health Monitor: RE 0 memory utilization
 jnxOperatingBuffer.9.1.0.0 52 active

32792 Health Monitor: Max Kernel Memory Used (%)
 jnxBoxKernelMemoryUsedPercent.0 3 active

32793 Health Monitor: jroute daemon memory usage
 Routing protocols process 51452 active
 Management process 38284 active
 Management process 38356 active
 Command-line interface 49108 active
 Periodic packet management process 9828 active
 Bidirectional Forwarding Detection process 13088 active
 Service Deployment Client 10012 active
 Event processing process 12692 active
 Layer 2 address flooding and learning process 20212 active
 MPLS Periodic Traceroute process 10488 active
 Multicast Snooping process 9608 active
 Feature license management process 12372 active

32794 Health Monitor: jkernel daemon memory usage
 Init daemon 1684 active
 Chassis control process 115888 rising threshold
 Firewall process 22584 active
 Interface control process 34000 active
 Simple Network Management Protocol process 21772 active
 Management Information Base II process 27848 active
 Alarm control process 12568 active
 Packet Forwarding Engine statistics management process 24388 active
 Craft interface I/O control process 13248 active
 Remote operations process 13712 active
 Class-of-service process 18908 active
 Internal routing service process 7924 active
 Inet process 6052 active
 USB supervise process 2388 active
 PPP process 8772 active
 Juniper Stateful Redundancy Protocol Daemon 13668 active
 Network security daemon 24248 active
 Simple Mail Transfer Protocol Client process 8088 active

```

	PFE relay process	8044 active
	Subscriber management process	17852 active
	Subscriber management helper process	21076 active
	Web management gatekeeper process	12820 active
	Application-identification process	18328 active
	IDP policy daemon	30188 active
	Shared memory routing socket message database process	15672 active
	System Health Management Daemon	15004 active
	Network security trace daemon	10400 active
	Wireless WAN process	15016 active
	Wireless LAN service process	13936 active
32797	Health Monitor: RE Temperature jnxFruTemp.9.1.0.0	51 active
32800	Health Monitor: RE Process count usage hrSystemProcesses.0	123 moderate threshold
32803	Health Monitor: RE Open file Descriptor count jnxHrSystemOpenFiles.0	738 active
32804	Health Monitor: FWDD Micro-Kernel threads total CPU Utilization jnxFwddMicroKernelCPUUsage.0	11 active
32805	Health Monitor: FWDD Real-Time threads total CPU Utilization jnxFwddRtThreadsCPUUsage.0	0 active
32806	Health Monitor: FWDD DMA Memory utilization jnxFwddDmaMemUsage.0	1 active
32807	Health Monitor: FWDD Heap utilization jnxFwddHeapUsage.0	39 active

## show snmp health-monitor routing-engine history

<b>Syntax</b>	<code>show snmp health-monitor routing-engine history resource &lt;cpu   memory   open-files-count   process-count   storage   temperature&gt;;</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D10 for branch SRX Series devices. Statement modified in Junos OS Release 12.1X45-D10.
<b>Description</b>	Display the health-monitoring information collected for a Routing Engine.
<b>Options</b>	<b>brief</b> —Displays brief health monitor history. <b>extensive</b> —Displays extensive health monitor history. <b>terse</b> —Displays terse health monitor history.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show snmp health-monitor on page 2090</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show snmp health-monitor routing-engine history on page 2097</a> <a href="#">show snmp health-monitor routing-engine history extensive on page 2098</a> <a href="#">show snmp health-monitor routing-engine history terse on page 2099</a>
<b>Output Fields</b>	Table 282 on page 2096 describes the output fields for the <b>show snmp health-monitor routing engine history</b> command. Output fields are listed in the approximate order in which they appear.

Table 282: show snmp health-monitor routing engine history Output Fields

Field Name	Field Description
<b>Resource</b>	Name of the health monitor object instance being monitored.
<b>Event</b>	Displays the latest event and time associated with the resource. The available events are: <ul style="list-style-type: none"> <li>Moderate Rising</li> <li>High Rising</li> <li>Critical Rising</li> <li>Moderate Falling</li> <li>High Falling</li> <li>Critical Falling</li> </ul>

Table 282: show snmp health-monitor routing engine history Output Fields (*continued*)

Field Name	Field Description
<b>Configuration</b>	Effective configuration of a resource. <ul style="list-style-type: none"> <li><b>interval</b> — Configured interval in seconds.</li> <li><b>moderate-threshold</b>—Percentage of moderate threshold level resource utilization.</li> <li><b>high-threshold</b> — Percentage of high-threshold level resource utilization.</li> <li><b>critical-threshold</b> — Percentage of critical threshold level resource utilization.</li> <li><b>action</b> — Configured action for a resource.</li> </ul>
<b>Usage Trail</b>	Displays the previous usage records.
<b>Top daemon</b>	List of processes with high resource utilization.
<b>Growing daemons</b>	List of processes with high incremental resource utilization from the previous sample.
<b>Top files</b>	List of large files in a partition.
<b>Growing files</b>	List of files in a partition that have gotten larger since the previous sample.
<b>Resource name</b>	Name of the resource.
<b>Latest event</b>	Displays the latest event associated with the resource. The available events are: <ul style="list-style-type: none"> <li>Moderate Rising</li> <li>High Rising</li> <li>Critical Rising</li> <li>Moderate Falling</li> <li>High Falling</li> <li>Critical Falling</li> </ul>
<b>Time elapsed</b>	Displays the time elapsed since the event occurred.
<b>Action</b>	Displays the action associated with the resource. The available actions are: <ul style="list-style-type: none"> <li>Monitor</li> <li>Prevent</li> <li>Recover</li> </ul>

## Sample Output

### show snmp health-monitor routing-engine history

```

user@host> show snmp health-monitor routing-engine history brief
Resource : CPU (jnxOperatingCPU.9.1.0.0)
Event : Critical Falling (76 %) 2013-04-10 18:44:47 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 76 76 76 78 78 78 78 78 78 78 ...
Top and Growing Consumer (%)
 Top Consumer Usage Growth
 flowd_octeon_hm 252 2

```

```

 idle: cpu0 34 34
 av_worker 3 2
 Growing Consumer Usage Growth
 idle: cpu0 34 34
 flowd_octeon_hm 252 2
 av_worker 3 2
 Load averages: 2.01 (1 min) 1.70 (5 min) 2.01 (15 min)

Resource : Var:/cf/var (jnxHrStoragePercentUsed.5)
Event : High Rising (70 %) 2013-04-10 14:51:29 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 70 70 69 69 69 69 69 69 69 69 ...
Top and Growing Consumer (KB)
 Top Consumer Usage Growth
 secdb_06.db 50424 0
 idpd_trace 23860 0
 SignatureUpdate.xml 20322 0
 ai_cachedfa_group_c 10784 0
 dfa_group_cache.db 10456 0
 Growing Consumer Usage Growth
 default-log-message 4403 4403
 chassisd 1467 4
 jsrpd 1202 2
 Storage used: 226034 KB, Inodes used: 506 Nodes

```

#### show snmp health-monitor routing-engine history extensive

```

user@host> show snmp health-monitor routing-engine history extensive
Resource : CPU (jnxOperatingCPU.9.1.0.0)
Event : Critical Falling (76 %) 2013-04-10 18:44:47 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 76 76 76 78 78 78 78 78 78 78 ...
Top and Growing Consumer (%)
 Top Consumer Usage Growth
 flowd_octeon_hm 252 2
 idle: cpu0 34 34
 av_worker 3 2
 Growing Consumer Usage Growth
 idle: cpu0 34 34
 flowd_octeon_hm 252 2
 av_worker 3 2
 Load averages: 2.01 (1 min) 1.70 (5 min) 2.01 (15 min)

Resource : CPU (jnxOperatingCPU.9.1.0.0)
Event : Critical Rising (85 %) 2013-04-10 18:43:28 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 85 85 85 84 84 84 84 84 84 84 ...
Top and Growing Consumer (%)
 Top Consumer Usage Growth
 flowd_octeon_hm 250 -1
 syshmd 14 0
 cli 8 0
 av_worker 2 0
 av_worker 1 0
 Load averages: 3.26 (1 min) 1.69 (5 min) 3.26 (15 min)

Resource : CPU (jnxOperatingCPU.9.1.0.0)
Event : High Rising (72 %) 2013-04-10 18:43:28 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 72 69 69 69 69 69 69 69 69 69 ...
Top and Growing Consumer (%)
 Top Consumer Usage Growth
 flowd_octeon_hm 251 4

```



```

init 14 14
syshmd 14 14
cli 8 8
av_worker 2 2
Growing Consumer Usage Growth
syshmd 14 14
init 14 14
cli 8 8
flowd_octeon_hm 251 4
av_worker 2 2
Load averages: 3.26 (1 min) 1.69 (5 min) 3.26 (15 min)

```

```

Resource : Var:/cf/var (jnxHrStoragePercentUsed.5)
Event : High Rising (70 %) 2013-04-10 14:51:29 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 70 70 69 69 69 69 69 69 69 ...
Top and Growing Consumer (KB)
Top Consumer Usage Growth
secdb_06.db 50424 0
idpd_trace 23860 0
SignatureUpdate.xml 20322 0
ai_cachedfa_group_c 10784 0
dfa_group_cache.db 10456 0
Growing Consumer Usage Growth
default-log-message 4403 4403
chassisd 1467 4
jsrpd 1202 2
Storage used: 226034 KB, Inodes used: 506 Nodes

```

```

Resource : Var:/cf/var (jnxHrStoragePercentUsed.5)
Event : Moderate Rising (65 %) 2013-04-10 14:16:42 JST
Configuration : 1/30/70/85/Monitor (Inter/Mod/High/Crit/Action)
Usage Trail (%): 65 ...
Top and Growing Consumer (KB)
Top Consumer Usage Growth
secdb_06.db 50424 0
idpd_trace 23860 0
SignatureUpdate.xml 20322 0
ai_cachedfa_group_c 10784 0
dfa_group_cache.db 10456 0
Growing Consumer Usage Growth
chassisd 1463 18
jsrpd 1200 7
Storage used: 211868 KB, Inodes used: 503 Nodes

```

### show snmp health-monitor routing-engine history terse

```
user@host> show snmp health-monitor routing-engine history terse
```

Resource name	Latest event	Time elapsed	Action
MD2:/mfs/var/run/utm	High Falling	00:00:36	Monitor
Root:/cf	Moderate Rising	1d 02:25	Monitor
Var:/cf/var	Critical Rising	00:02:38	Monitor
CPU	Critical Rising	1d 02:19	Monitor
Memory	Critical Rising	00:08:00	Monitor
RE process count	High Rising	1d 02:25	Monitor
RE open files count	Moderate Rising	1d 02:25	Monitor
RE Temperature	Moderate Rising	1d 02:24	Monitor

## show snmp health-monitor routing-engine status

<b>Syntax</b>	show snmp health-monitor routing-engine status;
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X45-D10 for branch SRX Series devices.
<b>Description</b>	Display the SNMP health-monitoring information for a Routing Engine.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show snmp health-monitor routing-engine history on page 2096</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show snmp health-monitor routing-engine status on page 2100</a>
<b>Output Fields</b>	Table 283 on page 2100 describes the output fields for the <b>show snmp health-monitor routing-engine status</b> command. Output fields are listed in the approximate order in which they appear.

**Table 283: show snmp health-monitor routing engine status Output Fields**

Field Name	Field Description
Alarm Index	Alarm identifier.
Resource name	Name of the resource.
Current State	Current state of the monitored variable.
Config Action	Displays the configured action.
Threshold	Displays the threshold value for medium, high, and critical as a percentage.
Interval	Displays the time taken in seconds.

## Sample Output

### show snmp health-monitor routing-engine status

```
user@host> show snmp health-monitor routing-engine status
```

```
Health monitor status
```

Alarm Index	Resource Name	Current State	Config Action	Threshold (M/H/C)%	Interval (sec)
32770	MD3:/jail/mfs	Active(47)	Monitor	70/80/90	1
32773	MD2:/mfs/var/run/utm	Moderate(69)	Monitor	70/80/90	1
32776	MD1:/mfs	Active(13)	Monitor	70/80/90	1
32782	Root:/cf	Moderate(54)	Monitor	30/70/85	1
32785	Config:/config	Active(0)	Monitor	30/70/85	1
32779	Var:/cf/var	Critical(85)	Monitor	30/70/85	1
32788	CPU	Critical(100)	Monitor	30/70/85	1

32791	Memory	Critical(88)	Monitor	70/80/90	1
32800	RE process count	High(81)	Monitor	30/70/85	1
32803	RE open files count	Moderate(58)	Monitor	30/70/85	1
32797	RE Temperature	Moderate(44)	Monitor	30/70/85	1

## show snmp mib (View)


<b>Syntax</b>	<code>show snmp mib (get   get-next   walk) (ascii   decimal) <i>object-id</i></code>
<b>Release Information</b>	Command introduced in Junos OS Release 9.4. Support for IPv4 and IPv6 systemwide policy statistics added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display local SNMP 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>
	<p> <b>NOTE:</b> On all high-end SRX Series devices, the <b>show snmp mib</b> command will not display the output for security related MIBs. We recommend that you use an SNMP client and prefix <b>logical-system-name@</b> to the community name. For example, if the community is public, use <b>default@public</b> for default root logical system.</p>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<p><a href="#">show snmp mib walk (standalone) on page 2103</a></p> <p><a href="#">show snmp mib walk (HA) on page 2103</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStats on page 2104</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStatsIPv4 on page 2104</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStatsTotalAllowIPv4Packets on page 2104</a></p>
<b>Output Fields</b>	<a href="#">Table 284 on page 2103</a> 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 284: 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 walk (standalone)

```
user@host> show snmp mib walk jnxJsSPUMonitoringObjectsTable
jnxJsSPUMonitoringFPCIndex.5 = 5
jnxJsSPUMonitoringSPUIndex.5 = 0
jnxJsSPUMonitoringCPUUsage.5 = 0
jnxJsSPUMonitoringMemoryUsage.5 = 61
jnxJsSPUMonitoringCurrentFlowSession.5 = 0
jnxJsSPUMonitoringMaxFlowSession.5 = 524288
jnxJsSPUMonitoringCurrentCPSession.5 = 0
jnxJsSPUMonitoringMaxCPSession.5 = 2359296
jnxJsSPUMonitoringNodeIndex.5 = 0
jnxJsSPUMonitoringNodeDescr.5 = single
```

### show snmp mib walk (HA)

```
user@switch> show snmp mib walk jnxJsSPUMonitoringObjectsTable
jnxJsSPUMonitoringFPCIndex.20 = 5
jnxJsSPUMonitoringFPCIndex.21 = 5
jnxJsSPUMonitoringFPCIndex.44 = 5
jnxJsSPUMonitoringFPCIndex.45 = 5
jnxJsSPUMonitoringSPUIndex.20 = 0
jnxJsSPUMonitoringSPUIndex.21 = 1
jnxJsSPUMonitoringSPUIndex.44 = 0
jnxJsSPUMonitoringSPUIndex.45 = 1
jnxJsSPUMonitoringCPUUsage.20 = 0
jnxJsSPUMonitoringCPUUsage.21 = 0
jnxJsSPUMonitoringCPUUsage.44 = 0
jnxJsSPUMonitoringCPUUsage.45 = 0
jnxJsSPUMonitoringMemoryUsage.20 = 64
jnxJsSPUMonitoringMemoryUsage.21 = 60
jnxJsSPUMonitoringMemoryUsage.44 = 64
jnxJsSPUMonitoringMemoryUsage.45 = 60
jnxJsSPUMonitoringCurrentFlowSession.20 = 0
jnxJsSPUMonitoringCurrentFlowSession.21 = 1
jnxJsSPUMonitoringCurrentFlowSession.44 = 0
jnxJsSPUMonitoringCurrentFlowSession.45 = 1
jnxJsSPUMonitoringMaxFlowSession.20 = 421888
jnxJsSPUMonitoringMaxFlowSession.21 = 843776
jnxJsSPUMonitoringMaxFlowSession.44 = 421888
jnxJsSPUMonitoringMaxFlowSession.45 = 843776
jnxJsSPUMonitoringCurrentCPSession.20 = 1
jnxJsSPUMonitoringCurrentCPSession.21 = 0
jnxJsSPUMonitoringCurrentCPSession.44 = 1
jnxJsSPUMonitoringCurrentCPSession.45 = 0
jnxJsSPUMonitoringMaxCPSession.20 = 2359296
jnxJsSPUMonitoringMaxCPSession.21 = 0
jnxJsSPUMonitoringMaxCPSession.44 = 2359296
```

```

jnxJsSPUMonitoringMaxCPSession.45 = 0
jnxJsSPUMonitoringNodeIndex.20 = 0
jnxJsSPUMonitoringNodeIndex.21 = 0
jnxJsSPUMonitoringNodeIndex.44 = 1
jnxJsSPUMonitoringNodeIndex.45 = 1
jnxJsSPUMonitoringNodeDescr.20 = node0
jnxJsSPUMonitoringNodeDescr.21 = node0
jnxJsSPUMonitoringNodeDescr.44 = node1
jnxJsSPUMonitoringNodeDescr.45 = node1

```

#### show snmp mib walk jnxJsPolicySystemStats

```

user@host> show snmp mib walk jnxJsPolicySystemStats
jnxJsPolicySystemStatsTotalAllowIPv4Packets.0 = 10347
jnxJsPolicySystemStatsTotalAllowIPv4Bytes.0 = 94053327
jnxJsPolicySystemStatsTotalAllowIPv4PacketsRate.0 = 21
jnxJsPolicySystemStatsTotalAllowIPv4BytesRate.0 = 1012
jnxJsPolicySystemStatsTotalDropIPv4Packets.0 = 257
jnxJsPolicySystemStatsTotalDropIPv4Bytes.0 = 40298
jnxJsPolicySystemStatsTotalDropIPv4PacketsRate.0 = 0
jnxJsPolicySystemStatsTotalDropIPv4BytesRate.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv4Flows.0 = 1
jnxJsPolicySystemStatsTotalAllowIPv4FlowsRate.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6Packets.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6Bytes.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6PacketsRate.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6BytesRate.0 = 0
jnxJsPolicySystemStatsTotalDropIPv6Packets.0 = 0
jnxJsPolicySystemStatsTotalDropIPv6Bytes.0 = 0
jnxJsPolicySystemStatsTotalDropIPv6PacketsRate.0 = 0
jnxJsPolicySystemStatsTotalDropIPv6BytesRate.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6Flows.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv6FlowsRate.0 = 0
jnxJsPolicySystemStatsEnabled.0 = 1

```

#### show snmp mib walk jnxJsPolicySystemStatsIPv4

```

user@host> show snmp mib walk jnxJsPolicySystemStatsIPv4
jnxJsPolicySystemStatsTotalAllowIPv4Packets.0 = 10347
jnxJsPolicySystemStatsTotalAllowIPv4Bytes.0 = 94053327
jnxJsPolicySystemStatsTotalAllowIPv4PacketsRate.0 = 21
jnxJsPolicySystemStatsTotalAllowIPv4BytesRate.0 = 1012
jnxJsPolicySystemStatsTotalDropIPv4Packets.0 = 257
jnxJsPolicySystemStatsTotalDropIPv4Bytes.0 = 40298
jnxJsPolicySystemStatsTotalDropIPv4PacketsRate.0 = 0
jnxJsPolicySystemStatsTotalDropIPv4BytesRate.0 = 0
jnxJsPolicySystemStatsTotalAllowIPv4Flows.0 = 1
jnxJsPolicySystemStatsTotalAllowIPv4FlowsRate.0 = 0

```

#### show snmp mib walk jnxJsPolicySystemStatsTotalAllowIPv4Packets

```

user@host> show snmp mib walk jnxJsPolicySystemStatsTotalAllowIPv4Packets
jnxJsPolicySystemStatsTotalAllowIPv4Packets.0 = 10347

```

## show system log-vital

<b>Syntax</b>	show system log-vital <data   oid   status>
<b>Release Information</b>	Command introduced in Junos OS Release 12.1X47-D15.
<b>Description</b>	Display the vital data of MIB OIDs.
<b>Options</b>	<b>data</b> —Display detailed vital data of the current day. <b>oid</b> —Display configured OID or group. <b>status</b> —Display the settings of the vital log.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">log-vital on page 2040</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system log-vital data on page 2106</a> <a href="#">show system log-vital oid on page 2107</a> <a href="#">show system log-vital status on page 2107</a>
<b>Output Fields</b>	<a href="#">Table 285 on page 2105</a> lists the output fields for the show system log-vital command. Output fields are listed in the approximate order in which they appear.

**Table 285: show system log-vital Output fields**

Field Name	Field Description
Node	Identification number of the node. It can be 0 or 1.
SPU	Identification of Services Processing Unit.
CPU	CPU usage of SPU in percentage.
Mem	Memory usage of SPU in percentage.
Flow-Sess	Number of flow sessions.
CP-Sess	Number of central point sessions.
IPv4-Sess	Number of IPv4 sessions.
IPv6-Sess	Number of IPv6 sessions.
CP-IPv4	Number of central point IPv4 sessions.
CP-IPv6	Number of central point IPv6 sessions.

Table 285: show system log-vital Output fields (*continued*)

Field Name	Field Description
OID list	OIDs that are being monitored.
OID number	Number of OIDs that are being monitored.
Group SPU list	SPUs that are being monitored.
Group SPU number	Number of SPU's that are being monitored.
Group screen list	Security zones whose screen stats are being monitored.
Group screen number	Number of security zones whose screen stats are being monitored.
Group	A set of OIDs. Once a group is enabled, all OIDs in the group are monitored.
interval	Number of minutes used for the data collection interval.
file-days	Number of days for the dump file to be stored.
storage-limit	Storage usage limit in percentage.
file-size	Size of the current dump file.
state	Number that indicates which state the current collection is in. It could indicate <b>IDLE</b> or <b>ONGOING</b> .
snmp mgmt-sock op number	Stat number of the querying MIB.
current timer counter	Number that indicates the collection timer.

## Sample Output

### show system log-vital data

```
user@host> show system log-vital data
```

```
#
Start firefly-perimeter--"fw1" Vitals Check Fri Sep 5 00:00:44 2014
#

[Fri Sep 5 00:00:44 2014] Vital data of SPU
Node SPU CPU Mem Flow-Sess CP-Sess IPv4-Sess IPv6-Sess
CP-IPv4 CP-IPv6
=====
node0 fwdd 0 55 10 0 10 0
0
0

#
End firefly-perimeter--"fw1" Vitals Check Fri Sep 5 00:00:45 2014
#
```



```
#
Start firefly-perimeter--"fw1" Vitals Check Fri Sep 5 00:01:45 2014
#

[Fri Sep 5 00:01:45 2014] Vital data of SPU
Node SPU CPU Mem Flow-Sess CP-Sess IPv4-Sess IPv6-Sess
CP-IPv4 CP-IPv6
=====
node0 fwdd 0 55 16 0 16 0
0 0

#
End firefly-perimeter--"fw1" Vitals Check Fri Sep 5 00:01:45 2014
#
```

### show system log-vital oid

```
user@host> show system log-vital oid

OID list:
lldpLocSysName.0 sys-name
 jnxJsNodeCurrentTotalSessIPv4.0 IPv4-sess-number
 .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 re cpu usage

OID number: 3
Group SPU list:
 All
Group SPU number: 1
Group screen list:
 trust
 untrust
Group screen number: 2
Group: idp cluster-counter storage operating
```

### show system log-vital status

```
user@host> show system log-vital status

log vital status:
interval: 1 Minutes
file-days: 4 days
storage-limit: 75 percent
file-size: 3 Mbytes
state: 5
snmp mgmt-sock op number: 0
current timer counter: 1 (vs 60)
```



## PART 7

# Standards Reference

- [Overview on page 2111](#)
- [Supported Standards on page 2113](#)



## CHAPTER 37

# Overview

- Accessing Standards Documents on page 2111

### Accessing Standards Documents

---

- Accessing Standards Documents on the Internet on page 2111

#### 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>.
- 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>.
- RFCs are published by the IETF. They can be accessed at <http://www.ietf.org/rfc.html>.



## CHAPTER 38

# Supported Standards

- [Chassis and System Standards on page 2113](#)
- [Interface Standards on page 2126](#)
- [Layer 2 Standards on page 2131](#)
- [MPLS Applications Standards on page 2133](#)
- [Packet Processing Standards on page 2138](#)
- [Routing Protocol Standards on page 2140](#)
- [Services PIC and DPC Standards on page 2153](#)
- [VPLS and VPN Standards on page 2157](#)

## Chassis and System Standards

---

- [Supported BOOTP and DHCP Standards on page 2113](#)
- [Supported Mobile IP Standards on page 2114](#)
- [Supported Network Management Standards on page 2115](#)
- [Supported RADIUS and TACACS+ Standards for User Authentication on page 2124](#)
- [Supported System Access Standards on page 2125](#)
- [Supported Time Synchronization Standard on page 2125](#)

## Supported BOOTP and DHCP Standards

The Junos OS substantially supports the following RFCs, which define standards for bootstrap protocol (BOOTP) and 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 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)*  
Address assignment is supported with IP version 4 (IPv4) but not IP version 6 (IPv6).
- 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 2111](#)

## Supported Mobile IP Standards

The Junos OS supports only static configuration of home agent addresses and IP tunnels; dynamic configuration is not supported. The 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).

The 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 2111](#)

## Supported Network Management Standards

The 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-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 **ipCidrRouteTable** [RFC 2096, *IP Forwarding Table 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).

- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

Only the **frDlcmiTable** object is supported.

- 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**
- **sysAppInstallElmtTable**
- **sysAppInstallPkgTable**
- **sysAppMapTable**
- 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*

Supported on J Series Services Routers. All MIB tables, objects, and traps applicable to the asymmetric digital subscriber line (ADSL) transceiver unit-remote (ATU-R) agent are supported.

- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2667, *IP Tunnel MIB*
- 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 2933, *Internet Group Management Protocol 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 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 4188, *Definitions of Managed Objects for Bridges*
- 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.

- Internet draft draft-ietf-idr-bgp4-mibv2-04.txt, *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**
- Internet draft draft-ietf-isis-wg-mib-07.txt, *Management Information Base for IS-IS*

Only the following tables are supported:

- **isisISAdjAreaAddrTable**
- **isisISAdjIPAddrTable**
- **isisISAdjProtSuppTable**
- **isisISAdjTable**
- 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*

**Related  
Documentation**

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported RADIUS and TACACS+ Standards for User Authentication

For validation of the identity of users who attempt to access a router, the Junos OS supports RADIUS authentication, TACACS+ authentication, and authentication by means of Junos user accounts configured on the router. The 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 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.

The 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 2125](#)
  - [Accessing Standards Documents on the Internet on page 2111](#)

## Supported System Access Standards

The 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 the Junos OS substantially supports SSH as an access protocol.

The Junos OS substantially supports RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*.

The Canada and U.S. version of the 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 2124](#)
  - [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Time Synchronization Standard

The 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.

- Related Documentation**
- [Accessing Standards Documents on the Internet on page 2111](#)

## Interface Standards

---

- [Supported ATM Interface Standards on page 2126](#)
- [Supported Ethernet Interface Standards on page 2126](#)
- [Supported Frame Relay Interface Standards on page 2127](#)
- [Supported GRE and IP-IP Interface Standards on page 2128](#)
- [Supported PPP Interface Standards on page 2128](#)
- [Supported SDH and SONET Interface Standards on page 2129](#)
- [Supported Serial Interface Standards on page 2130](#)
- [Supported T3 Interface Standard on page 2130](#)

### Supported ATM Interface Standards

The 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.

#### Related Documentation

- [Accessing Standards Documents on the Internet on page 2111](#)

### Supported Ethernet Interface Standards

The 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 802.1Qbb, *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 2111](#)

## Supported Frame Relay Interface Standards

The 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 2111](#)

## Supported GRE and IP-IP Interface Standards

The 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 2111](#)

## Supported PPP Interface Standards

The 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 2111](#)

## Supported SDH and SONET Interface Standards

The 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 2111](#)

## Supported Serial Interface Standards

The 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 2111](#)

## Supported T3 Interface Standard

The 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 2111](#)



## Layer 2 Standards

- [Supported Layer 2 Networking Standards on page 2131](#)
- [Supported L2TP Standards on page 2131](#)
- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 2 VPN Standard on page 2132](#)

### Supported Layer 2 Networking Standards

The 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 2131](#)
- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 2 VPN Standard on page 2132](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

### Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the 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

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Layer 2 Circuit Standards

The Junos OS substantially supports the following RFCs, which define standards for Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

The Junos OS does not support Section 5.3, “The Generalized PWid FEC Element.”

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*

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*

The 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 2157](#)
- [Supported Layer 2 VPN Standard on page 2132](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported Multicast VPN Standards on page 2159](#)
- [Supported VPLS Standards on page 2159](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Layer 2 VPN Standard

The Junos OS substantially supports Internet draft draft-kompella-ppvvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*.

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2157](#)
- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported Multicast VPN Standards on page 2159](#)
- [Supported VPLS Standards on page 2159](#)

- [Accessing Standards Documents on the Internet on page 2111](#)

## MPLS Applications Standards

---

- [Supported GMPLS Standards on page 2133](#)
- [Supported LDP Standards on page 2134](#)
- [Supported MPLS Standards on page 2135](#)
- [Supported RSVP Standards on page 2137](#)

## Supported GMPLS Standards

The 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 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, *Routing Extensions in Support of Generalized Multi-Protocol Label Switching*  
Only interface switching is supported.
- 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 2134](#)
- [Supported MPLS Standards on page 2135](#)
- [Supported RSVP Standards on page 2137](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## 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): Downstream Unsolicited mode is supported, but not Downstream on Demand mode.

- RFC 5443, *LDP IGP Synchronization*

**Related  
Documentation**

- [Supported GMPLS Standards on page 2133](#)
- [Supported MPLS Standards on page 2135](#)
- [Supported RSVP Standards on page 2137](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*

- RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

- RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

Only Point-to-Multipoint LSPs are supported.

- Internet draft draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*

- 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*

- Internet draft draft-ietf-mpls-soft-preemption-02.txt, *MPLS Traffic Engineering Soft preemption*

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*

Only the network element is supported.

- 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 2133](#)
- [Supported LDP Standards on page 2134](#)
- [Supported RSVP Standards on page 2137](#)

- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 2133](#)
- [Supported LDP Standards on page 2134](#)
- [Supported MPLS Standards on page 2135](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

---

## Packet Processing Standards

- [Supported CoS Standards on page 2138](#)
- [Supported Packet Filtering Standards on page 2139](#)
- [Supported Policing Standard on page 2139](#)

## Supported CoS Standards

The 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 2111](#)

## Supported Packet Filtering Standards

The 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**

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Policing Standard

The 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 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 2111](#)

---

## Routing Protocol Standards

- [Supported BGP Standards on page 2140](#)
- [Supported ES-IS Standards on page 2142](#)
- [Supported ICMP and Neighbor Discovery Standards on page 2143](#)
- [Supported IP Multicast Protocol Standards on page 2143](#)
- [Supported IPv4, TCP, and UDP Standards on page 2145](#)
- [Supported IPv6 Standards on page 2146](#)
- [Supported IS-IS Standards on page 2150](#)
- [Supported OSPF and OSPFv3 Standards on page 2151](#)
- [Supported RIP and RIPng Standards on page 2153](#)

### Supported BGP Standards

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 2146.

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 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 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 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 7311, *The Accumulated IGP Metric Attribute for BGP*

- Internet draft draft-ietf-idr-add-paths-04.txt, *Advertisement of Multiple Paths in BGP* (expires February 2011)
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- 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 2146](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported ES-IS Standards

The 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**

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported ICMP and Neighbor Discovery Standards

The Junos OS substantially supports the following RFCs, which define standards for 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 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

### Related Documentation

- [Supported IPv4, TCP, and UDP Standards on page 2145](#)
- [Supported IPv6 Standards on page 2146](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 4601, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 4607, *Source-Specific Multicast for IP*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
- *Using IGMPv3 and MLDv2 for Source-Specific Multicast*
- RFC 6513, *Multicast in MPLS/BGP IP VPNs*

- Internet draft draft-ietf-l3vpn-2547bis-mcast-bgp-08.txt, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- Internet draft draft-ietf-pim-sm-bsr-05.txt, *Bootstrap Router (BSR) Mechanism for PIM*

The scoping mechanism is not supported.

- Internet draft draft-raggarwa-l3vpn-2547-mvpn-00.txt, *Base Specification for Multicast in BGP/MPLS VPNs* (expires December 2004)

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 2111](#)

## Supported IPv4, TCP, and UDP Standards

The Junos OS substantially supports the following RFCs, which define standards for Internet Protocol 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 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)*

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 2146](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported IPv6 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for Internet Protocol version 6 (IPv6).

- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- 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 **inetCidrRouteTable** [RFC 4292, *IP Forwarding Table MIB*])



**NOTE:** RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.

- 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 1771, *A Border Gateway Protocol 4 (BGP-4)*



- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2375, *Multicast Address Assignments*
- RFC 2460, *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*

Internet Protocol 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 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 Internet Protocol version 4 (IPv4) but not Internet Protocol 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 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 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 5905, *Network Time Protocol Version 4 (for IPv6)*
- 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
- 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 the MP-BGP over Internet Protocol version 4 (IPv4) approach is supported.

#### Related Documentation

- [Supported IPv4, TCP, and UDP Standards on page 2145](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported IS-IS Standards

The 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 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*
- Internet draft draft-ietf-bfd-base-09.txt, *Bidirectional Forwarding Detection*  
Transmission of echo packets is not supported.
- Internet draft draft-ietf-isis-restart-02.txt, *Restart signaling for IS-IS*

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-bfd-base-09.txt, *Bidirectional Forwarding Detection* (except for the transmission of echo packets)
- Internet draft draft-ietf-isis-wg-255adj-02.txt, *Maintaining more than 255 circuits in IS-IS*

**Related  
Documentation**

- [Supported ES-IS Standards on page 2142](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 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 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 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 2146](#)
- [OSPF Overview](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 2145](#)
- [Supported IPv6 Standards on page 2146](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Services PIC and DPC Standards

---

- [Supported DTCP Standard on page 2153](#)
- [Supported Flow Monitoring and Discard Accounting Standards on page 2154](#)
- [Supported IPsec and IKE Standards on page 2154](#)
- [Supported L2TP Standards on page 2155](#)
- [Supported Link Services Standards on page 2155](#)
- [Supported NAT and SIP Standards on page 2156](#)
- [Supported RPM Standard on page 2156](#)
- [Supported Voice Services Standards on page 2157](#)

## Supported DTCP Standard

The 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 2111](#)

## 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, the 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*

### Related Documentation

- [Accessing Standards Documents on the Internet on page 2111](#)

## 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 the 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*
- RFC 2402, *IP Authentication Header*

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*
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- 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)*



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**

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the 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**

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Link Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the 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**

- [Accessing Standards Documents on the Internet on page 2111](#)

## 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, the 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.

The 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

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported RPM Standard

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the 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

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Voice Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the 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

- [Accessing Standards Documents on the Internet on page 2111](#)

---

## VPLS and VPN Standards

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2157](#)
- [Supported Layer 2 VPN Standard on page 2157](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported Multicast VPN Standards on page 2159](#)
- [Supported VPLS Standards on page 2159](#)

## Supported Carrier-of-Carriers and Interprovider VPN Standards

The Junos OS substantially supports the following RFCs and Internet draft, which define standards for carrier-of-carriers and interprovider virtual private networks (VPNs).

- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- Internet draft draft-marques-ppvnp-ibgp-00.txt, *RFC2547bis networks using internal BGP as PE-CE protocol*

### Related Documentation

- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 2 VPN Standard on page 2132](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported Multicast VPN Standards on page 2159](#)
- [Supported VPLS Standards on page 2159](#)
- [Supported BGP Standards on page 2140](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Layer 2 VPN Standard

The Junos OS substantially supports 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 2157](#)
  - [Supported Layer 2 Circuit Standards on page 2132](#)
  - [Supported Layer 3 VPN Standards on page 2158](#)
  - [Supported Multicast VPN Standards on page 2159](#)
  - [Supported VPLS Standards on page 2159](#)
  - [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Layer 3 VPN Standards

The 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 RFC does not define a standard, but provides information about technology related to Layer 3 VPNs. The IETF classifies it as a “Best Current Practice.”

- RFC 1918, *Address Allocation for Private Internets*

- Related Documentation**
- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2157](#)
  - [Supported Layer 2 Circuit Standards on page 2132](#)
  - [Supported Layer 2 VPN Standard on page 2132](#)
  - [Supported Multicast VPN Standards on page 2159](#)
  - [Supported VPLS Standards on page 2159](#)
  - [Supported MPLS Standards on page 2135](#)
  - [Supported BGP Standards on page 2140](#)
  - [OSPF Features in the Junos OS](#)

- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported Multicast VPN Standards

Junos OS substantially supports the following RFC and Internet draft, which define standards for multicast virtual private networks (VPNs).

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- Internet draft draft-ietf-l3vpn-2547bis-mcast-bgp-08.txt, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2157](#)
- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 2 VPN Standard on page 2132](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported VPLS Standards on page 2159](#)
- [Supported MPLS Standards on page 2135](#)
- [Supported BGP Standards on page 2140](#)
- [Accessing Standards Documents on the Internet on page 2111](#)

## Supported VPLS Standards

The Junos OS substantially supports the following following RFCs, 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.

### Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2157](#)
- [Supported Layer 2 Circuit Standards on page 2132](#)
- [Supported Layer 2 VPN Standard on page 2132](#)
- [Supported Layer 3 VPN Standards on page 2158](#)
- [Supported Multicast VPN Standards on page 2159](#)
- [Accessing Standards Documents on the Internet on page 2111](#)



## PART 8

# Index

- [Index on page 2163](#)





# Index

## Symbols

!	
in interface names.....	450
regular expression operator	
system logging.....	1729
" ", configuration group wildcards.....	465
#, comments in configuration statements.....	lvi, 360
\$	
regular expression operator	
system logging.....	1729
( )	
regular expression operator	
system logging.....	1729
( ), in syntax descriptions.....	lvi
*	
in interface names.....	449
regular expression operator.....	450
system logging.....	1729
wildcard character.....	465
* (red asterisk).....	588
+	
in statement lists.....	347
regular expression operator.....	450
system logging.....	1729
.	
regular expression operator	
system logging.....	1729
. (period)	
regular expression operator.....	450
/* */, comment delimiters.....	360
/cf/var/crash directory See crash files	
/cf/var/log directory See system logs	
/cf/var/tmp directory See temporary files	
/config/juniper.conf file.....	129
/config/juniper.conf.1 file.....	129
/config/rescue.conf file.....	129
/etc/config/factory.conf file.....	129
/var/log directory See system log messages	
/var/log/mib2d file.....	1969
/var/log/snmpd file.....	1969
< >, in syntax descriptions.....	lvi

?	
regular expression operator.....	465
system logging.....	1729
wildcard.....	465
? icon .....	588
[ ]	
regular expression operator	
system logging.....	1729
[ ], in configuration statements.....	lvi
\	
in interface names.....	449
wildcard characters.....	465
^	
regular expression operator	
system logging.....	1729
{ }, in configuration statements.....	lvi
specifying statements.....	395
regular expression operator	
system logging.....	1729
(pipe).....	548
command output.....	548
in syntax descriptions.....	lvi, 548
(pipe) command.....	1283
(pipe), in syntax descriptions.....	lvi, 548
A	
AAA Objects MIB.....	1819, 1831, 1836
Access Authentication Objects	
MIB.....	1819, 1826, 1831, 1837
access privilege levels	
configuration example.....	695
configuration mode hierarchies.....	698
operational mode commands.....	697
configuring.....	694
configuration mode hierarchies.....	697
operational mode commands.....	695
entering configuration mode.....	341
login classes.....	669
access privileges	
denying and allowing commands.....	666
permission bits for.....	664
predefined.....	663
specifying.....	674
access statement	
usage guidelines.....	1926
access, configuration summary.....	593
access-list statement.....	2010

accounting options		
configuration.....	1289	
configuration summary.....	593	
overview.....	1287	
sample task.....	616	
accounting profiles		
filter.....	1297	
interface.....	1295	
MIB.....	1307	
Routing Engine.....	1308	
accounting statement		
authentication		
usage guidelines.....	983	
Accounting-Options Configuration Statement		
Hierarchy.....	1552	
accounting-options statement.....	1557	
accounts See template accounts; user accounts		
action statement.....	1111	
action-profile statement.....	1558	
activate command.....	538	
usage guidelines.....	336	
activate statements and identifiers.....	358	
active configuration.....	304	
adaptive services interfaces		
alarm conditions and configuration		
options.....	1312	
Add new entry link.....	614	
address statement		
SNMPv3.....	2010	
usage guidelines.....	1939	
Address-Assignment Pool		
pool name.....	926	
Address-Assignment Pools.....	926	
address-assignment pools		
client attributes.....	956	
configuring overview.....	953	
DHCP attributes.....	956	
dhcpv6 attributes.....	956	
linking.....	956	
named range.....	955	
router advertisement.....	957	
address-assignment statement.....	1060	
address-mask statement.....	2011	
usage guidelines.....	1940	
address-pool statement.....	1063	
addresses		
machine name.....	312	
administrative roles		
example.....	682	
AES encryption		
setting.....	978	
agent, SNMP.....	1802	
agent-address statement.....	2011	
alarm class See alarm severity		
ALARM LED, color.....	1310	
Alarm MIB.....	1819, 1826, 1831, 1837	
alarm severity		
configuring for an interface.....	1316	
major (red) .....	1311	
See also major alarms		
minor (yellow).....	1311	
See also minor alarms		
alarm statement		
RMON.....	2012	
usage guidelines.....	1987	
alarms.....	1692	
active, displaying at login.....	1316	
chassis.....	628	
conditions, on an interface.....	1312	
configurable.....	1312	
configuration requirements for interface		
alarms.....	1316	
interface.....	628	
licenses.....	1315	
major.....	629, 1311 See major alarms	
minor.....	629, 1311 See minor alarms	
overview.....	1310	
red.....	629, 1311 See major alarms	
rescue configuration.....	1315	
severity.....	629, 1318, 1319 See alarm severity	
system.....	628	
type.....	628	
types.....	1311	
verifying.....	1318	
viewing, sample.....	629	
yellow.....	629, 1311 See minor alarms	
alarms sample task.....	629	
alert logging severity.....	632	
alias, CoS value.....	1389	
allow-commands statement		
usage guidelines.....	672	
allow-configuration statement.....	1064	
allow-configuration-regexps statement.....	1065	
usage guidelines.....	672	
allow-duplicates statement.....	1753	
allowing commands to login classes.....	672	
annotate command.....	336, 539	
usage guidelines.....	360	

- 
- ANSI standards supported See Index of Supported Software Standards
- any (system logging facility).....1718
- any (system logging severity level).....1719
- applications, configuration summary.....593
- apply-groups statement.....490
- usage guidelines.....459
- apply-groups-except statement.....490
- archive statement
- all system log files.....1754
- archive-sites statement
- accounting.....1559
- usage guidelines.....1294
- archiving files.....1174
- arithmetic and relational operators
- for monitor traffic command.....1616
- arithmetic operators, for multicast traffic.....1527
- AS path, displaying.....1425
- AT commands, for modem initialization
- description.....874
- ATM CoS MIB.....1820, 1831, 1837
- ATM interfaces
- supported software standards.....2126
- ATM MIB.....1820
- attacks
- brute force, preventing.....889
- dictionary, preventing.....889
- authentication
- local password, by default.....862
- login classes.....663, 674
- methods.....667, 673
- order of user authentication (configuration editor).....862
- RADIUS.....851
- RADIUS authentication (configuration editor).....855
- specifying a method.....862
- specifying access privileges.....674
- TACACS+.....857
- TACACS+ authentication (configuration editor).....859
- user accounts.....667, 674
- authentication-key statement.....1066
- authentication-md5 statement.....2013
- usage guidelines.....1924
- authentication-none statement.....2014
- usage guidelines.....1924
- authentication-order statement.....1067
- authentication-password statement.....2015
- usage guidelines.....1924
- authentication-sha statement.....2016
- usage guidelines.....1924
- authorization See permissions
- authorization (system logging facility).....1718
- authorization statement.....2017
- usage guidelines.....1902
- auto-configuration.....248, 249
- auto-prefix delegation.....963
- autoinstallation.....251
- automatic configuration process.....152
- CLI configuration editor.....154
- default configuration file.....152
- establishing.....151
- host-specific configuration file.....152
- interfaces.....152
- IP address procurement process.....152
- J-Web configuration editor.....154
- overview.....151
- protocols for procuring an IP address.....152
- requirements.....154
- status.....156
- TFTP server.....152
- verifying.....156
- autoinstallation, compatibility with the DHCP server.....923
- automatic configuration See autoinstallation
- ## B
- basic connectivity
- Quick Configuration.....609
- requirements.....609
- secure Web access.....865
- selecting.....627
- batch commit
- usage guidelines.....380, 381
- BFD MIB.....1820, 1827, 1831, 1837
- BGP
- supported software standards.....2140
- BGP (Border Gateway Protocol)
- monitoring.....1428
- peers, probes to See BGP RPM probes
- RPM probes to BGP neighbors See BGP RPM probes
- statistics.....1429
- BGP groups, displaying.....1429

BGP neighbors	
directing RPM probes to.....	1334
displaying.....	1429
monitoring with RPM probes.....	1332
BGP peers See BGP neighbors	
BGP routing information.....	1428
BGP RPM probes	
directing to select BGP neighbors	
(configuration editor).....	1334
overview.....	1324
setting up on local and remote device	
(configuration editor).....	1332
BGP sessions, status.....	1429
BGP4 V2 MIB.....	1820, 1826, 1831, 1837
binary operators, for multicast traffic.....	1527
binary security log file.....	1746
boot sequence.....	129
SRX Series devices.....	132
boot-server statement	
NTP.....	1068
bootp.....	252
BOOTP	
supported software standards.....	2113
BOOTP, for autoinstallation.....	154
braces, in configuration statements.....	lvi
brackets	
angle, in syntax descriptions.....	lvi
square, in configuration statements.....	lvi
branch SRX	
factory default	
configuration.....	8
licenses.....	35
reset.....	21
brief statement	
system logging.....	1772
usage guidelines.....	1724
broadcast messages, synchronizing NTP.....	1070
broadcast statement.....	1069
broadcast-client statement.....	1070
browser	
downloading software.....	139
browser interface See J-Web interface	
brute force attacks, preventing.....	889
built-in Ethernet ports See Ethernet ports;	
management interfaces	
buttons	
Cancel (J-Web configuration editor).....	590, 615
Commit (J-Web configuration	
editor).....	590, 615
Discard (J-Web configuration editor).....	615
OK (J-Web configuration editor).....	590, 615
Refresh (J-Web configuration editor).....	615
bypass LSPs, testing.....	1637
<b>C</b>	
Cancel button.....	615
J-Web configuration editor.....	590
candidate configuration.....	304
capture-file statement.....	1560
capturing packets See packet capture	
categories statement.....	2017
usage guidelines.....	1912
category change software installation.....	134
certificates See SSL certificates	
change-log (system logging facility).....	1718
chassis	
configuration summary.....	594
monitoring.....	644, 1452
power management.....	1452
chassis cluster.....	56
Chassis Cluster MIB.....	1821, 1832, 1837
chassis clusters	
redundancy group IP address monitoring	
configuration example.....	1354
Chassis Configuration Statement Hierarchy.....	1549
Chassis Definitions for Router Model MIB.....	1820
Chassis Forwarding MIB.....	1820
Chassis MIB.....	1820, 1827, 1832, 1837
checksum	
calculating for a file.....	1176, 1177, 1178
ciphers.....	1071
Class 1 MIB objects.....	1855
Class 2 MIB objects.....	1859
Class 3 MIB objects.....	1860
Class 4 MIB objects.....	1861
class of service (CoS)	
configuration summary.....	594
monitoring.....	637
Class-of-Service MIB.....	1821
class-usage-profile statement.....	1561
usage guidelines.....	1305
classifiers, CoS.....	1388, 1393
cleaning up files.....	625, 980, 981
clear chassis cluster ip-monitoring	
failure-count.....	1605
clear chassis cluster ip-monitoring failure-count	
ip-address.....	1606
clear dhcp client binding command.....	1163

- 
- clear dhcp client statistics command.....1164
  - clear dhcp relay binding command.....1165
  - clear dhcp relay statistics command.....1166
  - clear dhcp server binding command.....1167
  - clear dhcp server statistics command.....1168
  - clear dhcpv6 server binding command.....1171
  - clear dhcpv6 server statistics command.....1172
  - clear log command.....1781
  - clear security log file command.....1784
  - clear security logcommand.....1782
  - clear system login lockout command.....1173
  - clear system services dhcp conflicts
    - command.....922
  - cli.....13
  - CLI See Junos OS CLI
    - command completion.....522
    - command history.....331
      - displaying.....536
    - comparing configuration versions.....392
    - configuration mode
      - description.....335
      - navigation commands, table.....306
    - current working directory
      - displaying.....535
      - setting.....523
    - date
      - setting.....531
    - editing command line.....447
    - idle timeout, setting.....524
    - keyboard sequences.....448
    - permissions, displaying.....534, 1233
    - prompt strings.....484
    - prompt, setting.....525
    - restart, after software upgrade.....526
    - screen length, setting.....527
    - screen width, setting.....528
    - settings, displaying.....532
    - terminal type, setting.....529
    - timestamp.....484
    - timestamp, setting.....530
    - type checking.....397
    - users, monitoring.....421
    - word history.....331
    - working directory.....484
  - CLI configuration editor
    - autoinstallation.....154
    - controlling user access.....674
    - interface alarms.....1316
    - RADIUS authentication.....855
    - RPM.....1325
    - secure access configuration.....869
    - system log messages, sending to a file.....1748
    - TACACS+ authentication.....859
  - CLI terminal.....599
    - overview.....599
    - starting.....598
  - clickable configuration See J-Web configuration
    - editor
  - client attributes
    - address-assignment pools.....956
  - client list
    - adding to SNMP community.....1944
  - client-ia-type statement.....1073
  - client-identifier (dhcp-client) statement.....1073
  - client-identifier statement.....1074
  - client-list statement.....2018
    - usage guidelines.....1944
  - client-list-name statement.....1074, 2018
    - usage guidelines.....1944
  - client-type statement.....1075
  - clients statement.....2019
    - usage guidelines.....1902
  - cluster statement.....1562
  - code point aliases, CoS.....1389
  - command history
    - operational mode.....331
  - command output
    - configuration details.....365
    - configuration, comparing files.....439
    - end of, displaying from.....442
    - filtering
      - comparing configuration versions.....392
    - number of lines, counting.....441
    - pagination, preventing.....443
    - regular expressions
      - first match, displaying from.....442
      - matching output, displaying.....443
      - nonmatching output, ignoring.....441
    - retaining.....442
    - RPC, displaying.....441
    - saving to a file.....444
    - sending to users.....443
    - XML format, displaying.....441
  - command shell.....299
  - command-line interface See Junos OS CLI
    - downloading software.....139

commands		community statement	
allowing or denying to login classes.....	672	RMON.....	2021
completion.....	328, 485	usage guidelines.....	1991
configure.....	485	SNMP.....	2020
filenames, specifying.....	426	usage guidelines.....	1902
help about.....	325	community string, SNMP.....	1902
history.....	331	community-name statement.....	2022
options.....	417	usage guidelines.....	1946
URLs, specifying.....	426	compare command.....	548
comments		usage guidelines.....	392
adding to configuration file.....	360	compare filter.....	439
comments, in configuration statements.....	lvi	comparing files.....	1179
commit.....	253	completing partial command entry.....	522
commit and-quit command		compressing files.....	1174
usage guidelines.....	375	configuration	
commit at command		activating.....	390
usage guidelines.....	377	adding comments.....	360
Commit button.....	590, 615	autoinstallation of.....	151
commit command.....	540	candidate.....	304
usage guidelines.....	336, 372	committing.....	372, 615
commit comment command		and exiting configuration mode.....	375
usage guidelines.....	379	confirmation required.....	376
commit confirmed command		logging message about.....	379
usage guidelines.....	376	monitoring process.....	378
commit operations, pending		scheduling for later.....	377
displaying.....	572	synchronizing on Routing Engines.....	410
commit scripts.....	307	committing as a text file, with caution .....	597
commit statement.....	510	comparing with previous.....	392
commit synchronize command.....	540	deleting	
commit   display detail command		statements.....	348
usage guidelines.....	378	discarding changes .....	616
commit-delay statement.....	2019	displaying	
usage guidelines.....	1902	current configuration.....	564, 1647
commit-interval statement.....	491	details.....	365
committed configuration		downgrading software (CLI).....	178
comparing two configurations.....	623	downgrading software (J-Web).....	178
methods.....	621	downloading .....	623
overview.....	591, 612	edit command, using.....	346
storage location.....	592, 612	editing .....	593, 613
summaries.....	620	editing as a text file, with caution .....	597
committing a configuration.....	591, 612	global replacement.....	451
committing configuration		groups configuration groups See configuration	
and exiting configuration mode.....	375	groups	
basic.....	372	installation on multiple devices.....	151
confirmation required.....	376	loading previous .....	622
logging message about.....	379	locking.....	344
monitoring.....	378	merging current and new.....	399
scheduling for later.....	377	modifying.....	346
synchronizing on Routing Engines.....	410	previous, displaying.....	391

protecting.....	404	configuration mode, CLI.....	347, 372
replacing.....	399	command completion.....	328
rollback .....	622	commands	
saving to file.....	394	activate.....	336
storage of previous.....	389	annotate.....	336
unprotecting.....	404	commit.....	336
upgrading (CLI).....	173	copy.....	336
uploading .....	624	deactivate.....	336
users-editors, viewing.....	621	delete.....	336
validation.....	19	edit.....	336
verification.....	20	exit.....	336
viewing as a text file .....	595	extension.....	336
zones and policies.....	24	help.....	336
configuration database, summary.....	622	insert.....	336
configuration files		load.....	336
decrypting.....	977	paste.....	337
encrypting.....	977	quit.....	337
filename, specifying.....	426	rollback.....	322, 337
remote storage.....	130	run.....	337
saving to files.....	394	save.....	337
sequence of selection.....	129	set.....	337
URL, specifying.....	426	show.....	337
configuration groups		status.....	337
applying.....	459	top.....	337
creating.....	457	up.....	337
inheritance model.....	334	update.....	337
inherited values.....	463	configuration hierarchy, description.....	339
interface parameters.....	469, 471	description.....	335
nested groups.....	460	entering.....	341
overview.....	334	example .....	316
peer entities.....	472	exiting.....	342
re0, re1 groups.....	457	global replacement.....	451
regional configurations.....	474	identifier, description.....	338
sets of statements.....	468	locking.....	344
wildcards.....	465, 475	statement	
configuration hierarchy, J-Web display.....	589	container.....	339
configuration history		description.....	338
comparing files.....	623	leaf.....	339
database summary.....	622	switching to operational mode.....	311
downloading files.....	623	top level statements, interpreting.....	338
summary.....	620	users editing configuration	
users-editors, viewing.....	621	displaying.....	369
Configuration History page.....	620	multiple simultaneous users.....	375
Configuration Management		configuration mode, entering.....	543
MIB.....	1821, 1827, 1832, 1838	configuration sample tasks	
		accounting options.....	616
		configuration statements	
		adding comments about.....	360
		deleting.....	348

help about.....	327	CoS See class of service	
inheriting from groups.....	468	MIB.....	1821
overviews.....	346	supported software standards.....	2138
structure and components.....	395	CoS (class of service)	
configuration text		classifiers.....	1388, 1393
editing and committing, with caution.....	597	CoS value aliases.....	1389
viewing.....	595	forwarding classes.....	1390
configuration-servers.....	254	interfaces.....	1387
configure command.....	543	loss priority.....	1392
names and addresses.....	312	packet loss priority.....	1392
usage guidelines.....	341, 414	RED drop profiles.....	1390
configure exclusive command		rewrite rules.....	1391
usage guidelines.....	344	RPM probe classification.....	1329
configure link.....	614	See also TCP RPM probes; UDP RPM	
configuring address-assignment pool		probes	
dhcpv6.....	953	scheduler maps.....	1392
conflict-log (system logging facility).....	1718	CoS components for link services	
connecting device		applying on constituent links.....	1534
console port.....	15	count command.....	548
connections		count filter.....	441
testing		counters statement.....	1563
MPLS Layer 2 circuit connections.....	1623	crash files	
MPLS Layer 2 VPN connections.....	1626	cleaning up (CLI).....	981
MPLS Layer 3 VPN connections.....	1629	cleaning up (J-Web).....	980
MPLS LDP connections.....	1632	downloading (J-Web).....	983
MPLS LSP-endpoint connections.....	1635	crash files, cleaning up.....	625
MPLS RSVP connections.....	1637	critical logging severity.....	632
connectivity		curly braces, in configuration statements.....	lv
losing, after initial configuration.....	651	current working directory	
console port.....	13	displaying.....	535
disabling.....	888	setting.....	523
securing.....	888	cursor, moving.....	448
console statement		customer support.....	lvii
system logging.....	1756	contacting JTAC.....	lvii
usage guidelines.....	1725	system information, displaying.....	1208
contact statement.....	2023		
usage guidelines.....	1900	<b>D</b>	
container hierarchy See hierarchy		daemon (system logging facility).....	1718
Content Filtering		data plane logs.....	1745
verifying.....	1459	data types, CLI.....	397
control plane logs.....	1745	Database Information page.....	620
controlling user access.....	674	datapath-debug	
conventions		security.....	1564
text and syntax.....	lv	datapath-debug statement.....	1564
copy command.....	545	date	
usage guidelines.....	336, 414	setting from CLI.....	531
copying		days-to-keep-error-logs statement.....	491
files.....	1182	deactivate command.....	492
		usage guidelines.....	336



- 
- deactivate statements and identifiers
    - usage guidelines.....358
  - debug logging severity.....632
  - decryption-failures statement.....1565
  - default configuration
    - NAT.....5
    - policies.....5
  - default configuration file, for autoinstallation.....152
  - default configuration group.....481
  - default gateway
    - defining (Quick Configuration).....611
  - delete command.....493
    - usage guidelines.....336, 348
  - Delete Configuration Below This Point option
    - button.....616
  - delete link.....614
  - deleting
    - crash files (J-Web).....980
    - files.....1184
    - files, with caution.....982
    - licenses (CLI).....213, 1006
    - licenses (J-Web).....213, 1006
    - log files (J-Web).....980
    - temporary files (J-Web).....980
  - deny-commands statement
    - usage guidelines.....672
  - deny-configuration statement.....1075
  - deny-configuration-regexps statement
    - usage guidelines.....672
  - denying commands to login classes.....672
  - DES encryption
    - setting.....978
  - description statement
    - RMON.....2024
      - usage guidelines (alarms).....1988
      - usage guidelines (events).....1991
    - SNMP.....2023
      - usage guidelines.....1901
  - destination
    - NAT.....30
  - Destination Class Usage MIB.....1821, 1832, 1838
  - destination NAT
    - configuration.....30
    - verification.....34
  - destination statement.....1077
    - usage guidelines.....983
  - destination-classes statement.....1566
    - usage guidelines.....1305
  - destination-interface statement
    - RPM.....1567
  - destination-port statement
    - RPM.....1568
    - SNMP.....2024
      - usage guidelines.....1912
  - device
    - autoinstallation.....151
    - multiple, deploying See autoinstallation
    - packet capture.....1509
  - dfc (system logging facility).....1718
  - DHCP.....5
    - supported software standards.....2113
  - DHCP (Dynamic Host Configuration Protocol)
    - autoinstallation, compatibility with.....923
    - conflict detection and resolution.....922
    - interface restrictions.....922
    - monitoring.....643
    - options.....923
    - overview.....920
      - See also DHCP leases; DHCP pages; DHCP pools; DHCP server
    - server function.....920
    - verification.....933
  - DHCP Local Server
    - minimum configuration.....925
  - DHCP server
    - preparation.....924
    - sample configuration.....924
    - subnet and single client.....929, 938, 944, 970
    - verifying operation.....934
  - DHCP server, regaining lost lease.....651
  - dhcp-attributes statement IPv4.....1078
  - dhcp-attributes statement IPv6.....1080
  - dhcp-client attributes.....937
  - dhcp-client statement.....1081
  - dhcp-local-server.....1082
  - DHCPv6
    - configure server options.....950
  - dhcipv6.....1086
    - configuring address-assignment pool.....953
  - DHCPv6 client
    - identification.....958
    - minimum configuration.....960
    - optional attributes.....961
    - overview.....959
    - TCP/IP propagation.....965
  - DHCPv6 local server
    - overview.....949

dhcpcv6 security policy configuration.....	950	DiffServ code points, bits for RPM probes.....	1337
DHCPv6 server		directories	
preparation.....	950	working, displaying.....	535
dhcpcv6-client statement.....	1089	disable statement	
diagnosis		usage guidelines.....	359
alarm configurations.....	1318	disabling	
CLI command summary.....	1285	console port.....	888
displaying firewall filter for.....	1517	packet capture.....	1521
displaying packet capture configurations.....	1512	root login to console port.....	888
interfaces.....	1312, 1395	discard accounting	
J-Web tools overview.....	1285	supported software standards.....	2154
license infringement.....	1315	Discard All Changes option button.....	616
load balancing on the link services		Discard button.....	615
interface.....	1540	Discard Changes Below This Point option	
monitoring network performance.....	1321	button.....	616
MPLS connections (J-Web).....	1492	discarding configuration changes.....	616
network traffic.....	1523	disconnection of console cable for console	
packet capture.....	1509	logout.....	888
packet capture (J-Web).....	1527	display detail command	
packet encapsulation on link services		usage guidelines.....	365
interfaces.....	1539	display inheritance command	
ping command.....	1494	usage guidelines.....	463
ping host (J-Web).....	1496	display set command	
ping MPLS (J-Web).....	1492	usage guidelines.....	367
ports.....	1312	display xml filter.....	441
preparation.....	1494	displaying	
system logs.....	1744	licenses (J-Web).....	209, 1000
system operation.....	1485	d10.....	872
traceroute (J-Web).....	1486	dlv .....	1090
traffic analysis with packet capture.....	1509	DNS name resolution	
verifying captured packets.....	1512	troubleshooting.....	1533
verifying DHCP server operation.....	934	DNS Objects MIB.....	1821, 1832, 1838
verifying dialer interfaces.....	882	DNS server caching	
verifying RPM probe servers.....	1331	configuring TTL value.....	906
verifying RPM statistics.....	1328	DNS server, defining (Quick Configuration).....	611
diagnostic commands.....	1285	DNSSEC.....	1090
dial-in, USB modem		secure domains configuring.....	908
voice not supported.....	872	trusted keys configuring.....	908
dial-up modem connection		documentation	
connecting user end.....	886	comments on.....	lvii
dialer interface, for USB modem		domain name, defining (Quick Configuration).....	610
adding (configuration editor).....	879	domain search, defining (Quick Configuration).....	611
<i>See also</i> USB modem connections		downgrading	
verifying.....	882	software, with J-Web.....	178
dialer interface, USB modem		software, with the CLI .....	178
limitations.....	872	download URL.....	141
naming convention.....	872	downloading	
restrictions.....	872	configuration, with autoinstallation.....	152
dictionary attacks, preventing.....	889	crash files (J-Web).....	983

- licenses (J-Web).....209, 1001
  - log files (J-Web).....983
  - software upgrades.....141
  - temporary files (J-Web).....983
  - downloading configuration files .....623
  - downloading Junos OS.....138
  - drop probabilities, CoS.....1390
  - drop profiles, CoS.....1390
  - DS1 ports *See* T1 ports
  - DS3 ports *See* E3 ports; T3 ports
  - DSCPs (DiffServ code points), bits for RPM
    - probes.....1337
  - DTCP
    - supported software standards.....2153
  - dual-root partitioning.....169
  - dual-root partitioning scheme.....156
  - DVMRP
    - supported software standards.....2143
  - Dynamic Host Configuration Protocol *See* DHCP
- E**
- E3 ports, alarm conditions and configuration
    - options.....1312
  - edit command.....494
    - usage guidelines.....336
  - Edit Configuration page.....613
  - Edit Configuration Text page.....597
  - edit link.....614
  - edit security nat statement.....72
  - editing a configuration.....593
  - editing command line.....447
  - egress *See* RPM probes, outbound times
  - Emacs keyboard sequences.....447
  - emergency logging severity.....632
  - encapsulation overhead, PPP and MLPPP.....1539
  - encapsulation type
    - verifying for LFI and load balancing.....1539
  - encapsulation, modifying on packet
    - capture-enabled interfaces.....1522
  - encrypted access
    - through HTTPS.....865
    - through SSL.....865
  - engine-id statement
    - SNMPv3.....2025
    - usage guidelines.....1934
  - enterprise-oid statement.....2026
  - enterprise-specific MIBs, listed.....1826, 1830, 1836
  - enterprise-specific traps, SNMP
    - version 1.....1869
    - version 2.....1876
  - environment settings, CLI
    - command completion.....485
    - displaying.....485
    - example configuration.....485
    - idle timeout.....484
    - prompt string.....484
    - screen dimensions.....483, 486
    - software upgrade, restarting after.....484
    - terminal type.....484
    - timestamp.....484
    - working directory.....484
  - error logging severity.....632
  - ES-IS
    - supported software standards.....2142
  - ESO Consortium standards supported *See* Index of Supported Software Standards
  - Ethernet interfaces
    - supported software standards.....2126
  - Ethernet MAC MIB.....1827, 1832, 1838
  - Ethernet ports
    - alarm conditions and configuration
      - options.....1312
    - autoinstallation on.....152
    - configuring alarms on.....1316
  - Event MIB.....1821, 1827, 1833, 1838
  - event options, configuration summary.....594
  - event statement.....2026
    - usage guidelines.....1991
  - event viewer, J-Web
    - overview.....1447, 1750
    - See also* system log messages
  - event-rate statement.....1757
  - events
    - filtering.....632
    - filters.....632
    - overview.....630
    - regular expressions for filtering.....634
    - severity levels.....632
    - using.....630
    - viewing.....631
    - viewing, sample.....635
  - events sample task.....635
  - events statement
    - usage guidelines.....984
  - example
    - IP Monitoring.....1346

except command.....	548	file checksum sha-256 command.....	1178
except filter.....	441	file checksum sha1 command.....	1177
exclude statement.....	1758	file command.....	546
exclude-cmd-attribute statement.....	1143	usage guidelines.....	414, 423
exit command.....	495	file compare command.....	1179
from configuration mode.....	311	file copy command.....	1182
usage guidelines.....	336, 342	file delete command.....	1184
exit configuration-mode command.....	495	file encryption	
usage guidelines.....	342	decrypting configuration files.....	978
explicit-priority statement.....	1759	encrypting configuration files.....	978
usage guidelines		file list command.....	1185
single-chassis system.....	1725	file management	
extension command		configuration files.....	977
usage guidelines.....	336	crash files .....	625
		crash files (CLI).....	981
<b>F</b>		crash files (J-Web).....	980
facilities (system logging)		log files .....	625, 977
default for remote machine.....	1727	log files (CLI).....	981
for local machine.....	1718	log files (J-Web).....	980
facility-override statement.....	1759	packet capture file creation.....	1510
factory default configuration.....	5	temporary files .....	625
falling-event-index statement.....	2027	temporary files (CLI).....	981
usage guidelines.....	1988	temporary files (J-Web).....	980
falling-threshold statement		file rename command.....	1186
health monitor.....	2028	file show command.....	1187
usage guidelines.....	2000	file statement	
RMON.....	2029	accounting (associating with profile).....	1571
falling-threshold-interval statement		usage guidelines (filter profile).....	1298
RMON.....	2030	usage guidelines (interface profile).....	1296
usage guidelines.....	1989	usage guidelines (MIB profile).....	1307
family statement.....	1091	usage guidelines (Routing Engine	
FAQ (frequently asked questions)		profile).....	1309
Are LFI and load balancing working		accounting (configuring log file).....	1572
correctly?.....	1536	usage guidelines.....	1292
What causes jitter and latency on multilink		system logging.....	1761
bundles?.....	1536	usage guidelines.....	1723
Which CoS components apply on link services		filenames, specifying in commands.....	426
interface?.....	1534	files	
fe-0/0/0, defining address (Quick		archiving.....	1174
Configuration).....	611	calculating checksum.....	1176, 1177, 1178
feature licenses See licenses		comparing.....	1179
fields statement		compressing.....	1174
for interface profiles.....	1569	contents, displaying.....	1187
usage guidelines.....	1295	copying.....	1182
for Routing Engine profiles.....	1570	deleting.....	1184
usage guidelines.....	1309	list of, displaying.....	1185
file See security log		listing.....	424
file archive command.....	1174	log file, clearing.....	1781
file checksum md5 command.....	1176	renaming.....	1186

- saving command output to.....444
  - saving configurations to files.....394
  - status of, displaying.....1607, 1785
  - viewing.....423
- files statement.....1573, 1762
  - archiving of all system log files.....1754
- filter profile.....1297
- filter-duplicates statement.....2030
  - usage guidelines.....1904
- filter-interfaces statement.....2031
- filter-profile statement.....1573
  - usage guidelines.....1297
- filtering
  - command output.....1283
- filtering events
  - overview.....632
  - regular expressions.....634
- filtering get SNMP requests.....1904
- find command.....548
- find filter.....442
- FIPS See Junos-FIPS
- firewall.....55
- firewall (system logging facility).....1718
- firewall filters
  - configuration summary.....594
  - for packet capture, configuring.....1516
  - for packet capture, overview.....1510
  - monitoring.....641
  - sample task.....635
  - statistics
    - displaying.....112, 118, 1270
- Firewall MIB.....1821, 1827, 1833, 1838
- flags
  - login class.....669, 703
  - user permissions.....669
- flow monitoring
  - supported software standards.....2154
- flow statement
  - (Security Flow).....1574
- font conventions.....lv
- forwarding classes, CoS.....1390
- Forwarding Engine Board redundancy
  - monitoring.....645
- forwarding options, configuration summary.....594
- forwarding-options statement.....1095
- fragmentation, verifying on the link services
  - interface.....1538
- Frame Relay interfaces
  - supported software standards.....2127
- FreeBSD UNIX kernel.....300
- frequency, test See RPM probes, test intervals
- FRF (Broadband Forum) standards supported See Index of Supported Software Standards
- ftp (system logging facility).....1718
- fxp0, defining address (Quick Configuration).....611
- G**
  - ge-0/0/0, defining address (Quick Configuration).....611
  - Get requests, SNMP.....1800
  - global-threshold statement.....1576
  - global-weight statement.....1577
  - GMPLS
    - supported software standards.....2133
  - GR (Generic Requirements) standards supported See Index of Supported Software Standards
  - GRE interfaces
    - supported software standards.....2128
  - group licenses.....198, 990
  - group statement.....1096
    - SNMPv3 (for access privileges).....2033
    - usage guidelines.....1933
    - SNMPv3 (for configuring).....2032
    - usage guidelines.....1928
  - groups
    - BGP, displaying.....1429
  - Groups Configuration Statement Hierarchy.....1028
  - groups statement.....496
    - usage guidelines.....457
    - when.....518
- H**
  - halting a Services Router immediately.....627
  - hardware
    - major (red) alarm conditions on.....629, 1311
    - timestamp See RPM probe timestamps
  - hardware, major (red) alarm conditions
    - on.....629, 1311
  - hardware-timestamp statement.....1577
  - health-monitor statement.....2033
    - usage guidelines.....2000
  - heat status, checking.....1452
  - help apropos command
    - usage guidelines.....326
  - help command.....498, 547
    - usage guidelines.....326, 336
  - Help icon (?).....588, 590

help reference command	
usage guidelines.....	326
help syslog command	
usage guidelines.....	1735
help tip cli command	
usage guidelines.....	328
Help, J-Web interface.....	587, 590
history, CLI commands	
displaying.....	536
operational mode.....	331
hold command.....	548
hold filter.....	442
host (Security Logging) statement.....	1763
host reachability	
ping command.....	1494
ping host (J-Web).....	1496
Host Resources MIB.....	1822, 1827, 1833, 1838
host statement	
ssh-known-hosts.....	1099
host-specific configuration file, for	
autoinstallation.....	152
hostkey-algorithm.....	1100
hostname	
monitoring traffic by matching.....	1525
opening an SSH session to.....	899
pinging (CLI).....	1495
pinging (J-Web).....	1497
resolving.....	924
telnetting to.....	898
tracing a route to (CLI).....	1360, 1490
tracing a route to (J-Web).....	1487
hostname, defining (Quick Configuration).....	610
hostname.conf file, for autoinstallation.....	152, 154
hosts, reachability	
MPLS Layer 2 circuits.....	1623
MPLS Layer 2 VPN connections.....	1626
MPLS Layer 3 VPN connections.....	1629
MPLS LDP LSPs.....	1632
MPLS LSP endpoints.....	1635
MPLS RSVP LSPs.....	1637
HTTP (Hypertext Transfer Protocol)	
enabling Web access.....	606, 868
enabling Web access (configuration editor).....	869
on built-in management interfaces.....	605, 865
verifying configuration.....	871
HTTP (Hypertext Transfer Protocol), RPM probes.....	1321
httpd process, limiting subordinate processes.....	649
HTTPS (Hypertext Transfer Protocol over SSL)	
enabling secure access.....	606, 868
enabling secure access (configuration editor).....	869
J-Web configuration.....	868
recommended for secure access.....	605, 865
verifying secure access configuration.....	871
HTTPS Web access, establishing.....	865
Hypertext Transfer Protocol See HTTP	
Hypertext Transfer Protocol over SSL See HTTPS	
Hypertext Transfer Protocol, RPM probes.....	1321
I	
IANA standards supported See Index of Supported Software Standards	
ICMP	
supported software standards.....	2143
ICMP (Internet Control Message Protocol)	
RPM probes, description.....	1321
RPM probes, inbound and outbound times.....	1323
RPM probes, setting.....	1325
icmp statement	
RPM.....	1578
identifier link.....	614
identifiers	
inserting in sequential lists.....	352
renaming.....	351
specifying.....	395
idle timeout	
user, setting.....	524
values, CLI sessions.....	484
IDP.....	49
configuration.....	50
recommended	
policy.....	49
template.....	49
verification.....	54
IDP MIB.....	1822, 1830
idp potential violation statement.....	1578
IEEE standards supported See Index of Supported Software Standards	
IGMP	
supported software standards.....	2143
ignore filter.....	441
IKE	
supported software standards.....	2154

- 
- ILMI.....1799
  - inbound time See RPM probes
  - INCITS standards supported See Index of Supported Software Standards
  - info logging severity.....632
  - informs SNMP See SNMP informs
  - ingress See RPM probes, inbound times
  - inheritance model, configuration groups.....334
  - inherited values, configuration groups.....463
  - init-command-string command.....874
  - initial configuration requirements.....609
  - insert command.....499
    - usage guidelines.....336, 352
  - Install Remote page
    - field summary.....162, 176
  - installation
    - licenses (CLI).....210, 1003
    - licenses (J-Web).....210, 1003
    - software upgrades (CLI).....173
    - software upgrades, from a remote server.....175
    - software upgrades, uploading.....173
  - installation packages.....126
  - installation types.....133
  - Instance to which this connection belongs
    - description.....1492
    - using.....1500
  - integrated local management interface See ILMI
  - interactive-commands (system logging facility).....1718
  - interface
    - configuration example.....316
  - Interface MIB.....1822, 1828, 1833, 1839
  - interface names
    - conventions.....422
  - interface profile.....1295
  - interface statement.....1101
    - SNMP.....2034
      - usage guidelines.....1905
  - interface-profile statement.....1579
    - usage guidelines.....1295
  - interface-traceoptions statement
    - DHCP local server.....1104
  - interfaces See management interfaces; network
  - interfaces; ports
    - configuration summary.....594
    - media parameters.....469, 471
    - monitoring.....637
  - interfaces (ARP).....1102
  - interfaces (autoinstallation).....255
  - Interfaces Configuration Statement
    - Hierarchy.....1012
  - interfaces limiting SNMP access.....1905
  - interfaces statement.....1103
  - internet.....17
  - 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.....2135
  - Internet draft
    - draft-napierala-mpls-targeted-mldp-01.txt, Using LDP Multipoint Extensions on Targeted LDP Sessions .....2134
  - Internet drafts supported See Index of Supported Software Standards
  - Internet Explorer, modifying for worldwide version of Junos OS.....581, 604
  - internet service provider (isp).....14
  - interval statement
    - accounting.....1580
      - usage guidelines (filter profile).....1298
      - usage guidelines (interface profile).....1296
      - usage guidelines (MIB profile).....1307
      - usage guidelines (Routing Engine profile).....1309
    - health monitor.....2035
      - usage guidelines.....2000
    - RMON.....2034
      - usage guidelines.....1989
  - intervals, probe and test See RPM probes
  - intrusion detection and prevention.....49
  - IP Forward MIB.....1822, 1828, 1833, 1839
  - IP Monitoring.....1344, 1346
    - route failover.....1344
    - supported threshold.....1345
    - test parameter.....1345
  - IP multicast
    - supported software standards.....2143
  - tracing routes
    - listen for responses.....1621
  - IP-IP interfaces
    - supported software standards.....2128
  - ip-monitoring statement.....1581
  - ipconfig command.....934
    - explanation.....934
  - IPsec.....56
    - supported software standards.....2154
  - IPsec Generic Flow Monitoring Object
    - MIB.....1822, 1828, 1833, 1839



IPsec Monitoring MIB.....	1822, 1828, 1833, 1839
IPsec tunnels	
monitoring.....	642
IPsec VPN Objects MIB.....	1822
IPv4	
supported software standards.....	2145
IPv4 MIB.....	1823, 1828, 1834, 1839
IPv6	
supported software standards.....	2146
IPv6 and ICMPv6 MIB.....	1823
IPv6 SNMP community string.....	1903
IS-IS	
supported software standards.....	2150
ISO/IEC standards supported See Index of Supported Software Standards	
issuing relative configuration commands.....	351
ITU-T Recommendations supported See Index of Supported Software Standards	
<b>J</b>	
J-web.....	13
J-Web configuration	
adding users.....	674
authentication method.....	862
J-Web Configuration	
secure Web access.....	868
J-Web configuration editor	
autoinstallation.....	154
committing a configuration.....	615
configuration hierarchy display.....	589
configuration text, viewing.....	595
controlling user access.....	674
editing a configuration.....	613
interface alarms.....	1316
RADIUS authentication.....	855
RPM.....	1325
secure access.....	869
system log messages, sending to a file.....	1748
TACACS+ authentication.....	859
J-Web graphical user interface (GUI).....	307
J-Web interface	
comparing configuration differences.....	623
context-sensitive help.....	587
Diagnose options.....	1285
event viewer.....	635, 1447, 1750
Help (?) icon.....	588
Internet Explorer, modifying for worldwide version of Junos OS.....	581, 604
layout.....	587
losing connectivity after initial configuration.....	651
main pane.....	588
managing licenses.....	197, 990
overview.....	301, 577, 579, 591
page layout.....	583, 587
sessions.....	586
side pane.....	589
starting.....	581, 604
top pane.....	587
unpredictable results, multiple windows.....	651
windows, multiple, unpredictable results with.....	586
J-Web Quick Configuration See Quick Configuration	
J-Web software, installing.....	603
jitter	
description.....	1323
<i>See also</i> RPM probes	
in RPM probes, improving with timestamps.....	1322
monitoring.....	1340
threshold, setting.....	1337
jitter, removing on multilink bundles.....	1536
jnxRmonAlarmTable.....	1985
Juniper Networks MIB objects.....	1851
juniper-ais configuration group	
usage guidelines.....	458
Junos OS	
autoinstallation.....	151
configuration files.....	129
downloading.....	138
editions.....	124
Canada and U.S.....	124
Junos-FIPS.....	124, 125
worldwide.....	124
generating licenses.....	209, 1001
information security.....	127
installation	
current configuration, confirming.....	137
PIC combinations, verifying.....	137
installation packages.....	126
Internet Explorer, modifying for worldwide version.....	581, 604
introduction.....	123
naming convention.....	126
packages	
digital signatures.....	127
MD5 checksum.....	127



- naming conventions.....128
    - SHA-1 checksum.....127
    - release naming conventions.....128
    - release numbers.....128
    - software installation types.....133
    - storage media
      - device names.....132
    - upgrading.....169
    - version, displaying.....138
    - worldwide version, modifying Internet Explorer
      - for.....581, 604
  - Junos OS CLI.....599
    - access privilege levels.....664
    - command modes.....303, 580, 600
    - denying and allowing commands.....666
    - diagnostic command summary.....1286
    - filtering command output.....1283
    - overview.....303, 580, 599
    - See also CLI terminal
  - Junos OS versions See Junos OS editions
  - Junos Scope application.....301, 578
  - Junos XML management protocol.....307
    - enabling secure access.....868
    - verifying secure access configuration.....871
  - Junos XML protocol over SSL.....868
  - junos-defaults configuration group.....571
    - displaying.....481, 567, 571
  - Junos-FIPS.....125
    - installation and configuration
      - requirements.....125
    - password requirements.....125, 667
  - Junos-FIPS software environment.....307
  - JUNOScript
    - enabling secure access.....606
  - JUNOScript API
    - defining access (Quick Configuration).....611
  - JUNOScript over SSL.....606
- K**
- kernel (system logging facility).....1718
  - key performance indicators.....1997
  - keyboard sequences
    - editing command line.....447
- L**
- L2TP
    - supported software standards.....2131, 2155
  - label-switched paths See LSPs
  - LAN.....5
  - laptop See management device
  - last command.....548
  - last filter.....442
  - latency, in RPM probes, improving with
    - timestamps.....1322
  - latency, reducing on multilink bundles.....1536
  - Layer 2 circuits
    - reachability, testing.....1623
    - supported software standards.....2132
  - Layer 2 circuits, monitoring.....1492
  - Layer 2 networking
    - supported software standards.....2131
  - Layer 2 VPNs
    - reachability, testing.....1626
  - Layer 2 VPNs, monitoring.....1492
  - Layer 3 VPNs
    - reachability, testing.....1629
  - Layer 3 VPNs, monitoring.....1492
  - layout, J-Web.....587
  - LDP
    - supported software standards.....2134
  - LDP LSPs
    - ping interval.....1632
  - lease-time (dhcp-client) statement.....1107
  - libpcap format, for packet capture files.....1512
  - license infringement
    - identifying any licenses needed.....197, 990
    - verifying license usage.....213, 1005
    - verifying licenses
      - installed.....212, 214, 1005, 1007
  - license keys
    - components.....197, 989
    - displaying (CLI).....213, 1006
    - status.....197, 990
    - version.....197, 990
  - License MIB.....1823, 1828, 1834, 1839
  - licenses.....35
    - adding (CLI).....210, 1003
    - adding (J-Web).....210, 1003
    - deleting (CLI).....213, 1006
    - deleting (J-Web).....213, 1006
    - displaying.....115, 287, 1266
    - displaying (CLI).....212, 214, 1005, 1007
    - displaying (J-Web).....197, 209, 990, 1000
    - displaying usage.....213, 1005
    - downloading (J-Web).....209, 1001
    - generating.....209, 1001
    - group.....198, 990

infringement, preventing.....	197, 990	load merge command	
See also license infringement		usage guidelines.....	399
key.....	197, 989	load override command	
See also license keys		usage guidelines.....	399
managing (J-Web).....	197, 990	load set command	
overview.....	195, 196, 989	usage guidelines.....	400
saving (CLI).....	210, 1002	loading a configuration file	
updating (CLI).....	210, 1003	downloading .....	623
verifying.....	212, 214, 1005, 1007	rollback .....	622
licenses, alarm conditions and remedies.....	1315	uploading .....	624
limit statement		local password	
cache		default authentication method for	
security log.....	1763	system.....	862
limitations		method for user authentication .....	862
ALARM LED lights yellow whether alarm is		order of user authentication (configuration	
minor or major.....	1310	editor).....	862
DHCP, no support on VPN interfaces.....	922	overview.....	667, 673
MPLS, no LSP statistics on outbound		local template accounts.....	677
device.....	1403	local-engine statement.....	2036
mtrace from-source packet statistics always		Locate LSP from interface name	
0.....	1358	description.....	1492
performance degradation with monitor traffic		using.....	1500
command.....	1523	Locate LSP from virtual circuit information	
PPP, no J-Web monitoring information		description.....	1492
available.....	1406	using.....	1500
Server relay and DHCP client cannot coexist in		Locate LSP using interface name	
device.....	920	description.....	1492
software downgrade cannot be undone.....	178	using.....	1500
unpredictable behavior with multiple		location statement	
windows.....	651	SNMP.....	2037
link services		usage guidelines.....	1900
supported software standards.....	2155	locking configuration.....	344
link services interface		lockout-period statement.....	1109
applying CoS components on constituent		log.....	1782
links.....	1534	Services .....	1764
fragmentation, troubleshooting.....	1538	log file.....	1784
load balancing, troubleshooting.....	1540	log files	
MLPPP header overhead.....	1539	archiving.....	977
packet encapsulation, troubleshooting.....	1539	clearing contents of.....	1781
PPP header overhead.....	1539	contents, displaying.....	1789
reducing jitter and latency on multilink		deleting unused files.....	977
bundles.....	1536	display of	
troubleshooting LFI and load balancing.....	1536	starting.....	1608, 1786
load balancing on link services interfaces		stopping.....	1610, 1788
FAQ.....	1536	rotating.....	977
troubleshooting.....	1536	status, displaying.....	1607, 1785
verifying.....	1540	log messages See system log messages	
load command.....	500		
usage guidelines.....	336		

- log-prefix statement
    - system logging.....1765
    - usage guidelines.....1732
  - log-rotate-frequency statement.....1765
  - log-vital.....2040
  - logging severity levels.....632
  - logical interfaces
    - unit numbers.....423
  - logical interfaces, CoS.....1387
  - logical operators
    - for monitor traffic command.....1614
  - logical operators, for multicast traffic.....1526
  - Logical Systems MIB.....1823, 1834, 1839
  - logical-system statement.....2038
  - logical-system-trap-filter statement.....2039
  - login classes
    - access privilege levels.....669
    - commands, allowing or denying.....672
    - defining (configuration editor).....674
    - permission bits for.....664
    - predefined permissions.....663
    - specifying.....674
  - login lockout.....1173, 1269
  - login retry limits, setting.....889
  - logs See system logs
  - loopback address, defining (Quick Configuration).....611
  - loss priority, CoS.....1392
  - LSPs
    - LDP, ping interval.....1632
    - RSVP, ping interval.....1637
  - LSPs (label-switched paths)
    - information about.....1402
    - monitoring, with ping MPLS.....1492
    - statistics.....1403
  - LSYS MIB.....1823
- M**
- macs.....1110
  - main pane, J-Web.....588
  - major (red) alarms.....629
    - description.....1311
  - Management Access page
    - description.....606
  - management device
    - diagnosing problems from.....1284
    - monitoring from.....636, 1283
    - recovering root password from.....1532
  - Management Information Base See MIBs
  - management interface address, defining (Quick Configuration).....611
  - management interfaces
    - alarm conditions and configuration
      - options.....1312
    - configuring alarms on.....1316
    - monitoring.....1395, 1400
    - statistics.....1395
  - managing
    - files.....977
    - software.....169
    - user authentication.....673
  - manuals
    - comments on.....lvii
  - master agent, SNMP.....1802
  - match command.....548
  - match conditions
    - for monitor traffic command.....1613
  - match conditions, for multicast traffic
    - .....1525
  - match filter.....443
  - match statement.....1766
    - usage guidelines.....1728
  - maximum-aggregate-pool statement.....501
  - maximum-capture-size
    - security log.....1583
  - maximum-entries statement.....502
  - MD5 (Message Digest 5) checksum.....127
  - MD5 checksum, calculating.....1176
  - message-processing-model statement.....2042
    - usage guidelines.....1942
  - messages See system log messages
    - broadcast messages, NTP.....1070
  - MIB profile.....1307
  - mib-profile statement.....1583
    - usage guidelines.....1307
  - MIBs
    - AAA Objects.....1819, 1831, 1836
    - Access Authentication
      - Objects.....1819, 1826, 1831, 1837
    - Alarm.....1819, 1826, 1831, 1837
    - ATM.....1820
    - ATM CoS.....1820, 1831, 1837
    - BFD.....1820, 1827, 1831, 1837
    - BGP4 V2.....1820, 1826, 1831, 1837
    - Chassis.....1820, 1827, 1832, 1837
    - Chassis Cluster.....1821, 1832, 1837
    - Chassis Definitions for Router Model.....1820
    - Chassis Forwarding.....1820

Class-of-Service.....	1821
Configuration	
Management.....	1821, 1827, 1832, 1838
Destination Class Usage.....	1821, 1832, 1838
DNS Objects.....	1821, 1832, 1838
enterprise-specific, listed.....	1826, 1830, 1836
Ethernet MAC.....	1827, 1832, 1838
Event.....	1821, 1827, 1833, 1838
Firewall.....	1821, 1827, 1833, 1838
Host Resources.....	1822, 1827, 1833, 1838
IDP.....	1822
Interface.....	1822, 1828, 1833, 1839
IP Forward.....	1822, 1828, 1833, 1839
IPsec Generic Flow Monitoring Object	
.....	1822, 1828, 1833, 1839
IPsec Monitoring.....	1822, 1828, 1833, 1839
IPsec VPN Objects.....	1822
IPv4.....	1823, 1828, 1834, 1839
IPv6 and ICMPv6.....	1823
License.....	1823, 1834
license.....	1828, 1839
Logical Systems.....	1823
logical systems.....	1834, 1839
LSYS.....	1823
Multicast.....	1809, 1810, 1818
NAT Objects.....	1823, 1828, 1834, 1840
OSPF.....	1806
Packet Forwarding	
Engine.....	1823, 1829, 1834, 1840
Ping.....	1823, 1829, 1834, 1840
use in ping test.....	1962
view configuration example, SNMP.....	1907
Policy Objects.....	1824, 1829, 1834, 1840
PPP.....	1806
Reverse-Path-Forwarding.....	1824, 1829, 1834, 1840
RMON Events and Alarms	
.....	1824, 1829, 1835, 1840
Security Interface Extension	
Objects.....	1824, 1829, 1835, 1841
Security Screening Objects.....	1824, 1835, 1841
SNMP IDP.....	1822, 1830
SNMP object values, displaying.....	2102
Source Class Usage.....	1824, 1835, 1841
SPU Monitoring.....	1825, 1835
SPU monitoring.....	1841
Structure of Management	
Information.....	1825, 1826, 1831
Junos OS for SRX Series devices,	
for.....	1826, 1831, 1836
System Log.....	1825, 1830, 1835, 1841
Traceroute.....	1825, 1830, 1836, 1841
Utility.....	1825, 1830, 1836, 1841
views	
SNMP.....	1906
VPN.....	1826
VPN Certificate	
Objects.....	1825, 1830, 1836, 1842
minimum accounting options configuration.....	1290
minor (yellow) alarms.....	629
description.....	1311
MLD	
supported software standards.....	2143
MLPPP encapsulation, on the link services	
interface.....	1539
Mobile IP	
supported software standards.....	2114
mode (Security Logging) statement.....	1766
modem connection to router USB port	
connecting USB modem to router.....	875
monitor interface command.....	1395
controlling output.....	1395
monitor interface traffic command.....	1395
controlling output.....	1395
monitor list command.....	1485, 1607, 1785
monitor sample task.....	645, 647
monitor start command.....	1485, 1608, 1786
monitor stop command.....	1485, 1610, 1788
monitor traffic command.....	1523, 1611
options.....	1523
performance impact.....	1523
monitor traffic matching command.....	1523
arithmetic, binary, and relational	
operators.....	1527
logical operators.....	1526
match conditions.....	1525
monitoring	
BGP.....	1429
BGP neighbors, with RPM probes.....	1332
chassis.....	644, 1452
class of service.....	637
CLI commands and corresponding J-Web	
options.....	636
DHCP.....	643
FEB redundancy.....	645
firewall filters.....	641
interfaces.....	637, 1395, 1400
interfaces, sample.....	645
IPsec.....	642

- J-Web tasks and corresponding CLI
  - commands.....636
- Layer 2 circuits.....1492
- Layer 2 VPNs.....1492
- Layer 3 VPNs.....1492
- MPLS.....638
- MPLS traffic
  - engineering.....1401, 1402, 1403, 1404, 1405
- NAT.....642
- network interface traffic.....1523
- network traffic with packet capture.....1509
- OSPF.....1427
- overview.....636
  - See also diagnosis; statistics; status
- ports.....1400
- PPP (CLI).....1406
- PPPoE.....1407
- preparation.....1494
- Process Details.....645
- RIP.....1426
- route information, sample.....647
- routing.....640
- routing information.....1423
- routing tables.....1423
- RPM.....639
- RPM probes.....1340
- service quality.....1996
- service sets.....643
- system.....644
- system log messages.....1744
- system logs.....1485
- trace files.....1485
- monitoring the wx interface.....1411
- MPLS
  - Layer 2 circuit connections
    - operability, checking.....1623
  - Layer 2 VPN connections
    - operability, checking.....1626
  - Layer 3 VPN connections
    - operability, checking.....1629
  - LDP-signaled LSP connections
    - operability, checking.....1632
  - LSP endpoint connections
    - operability, checking.....1635
  - standard traps.....1890
  - supported software standards.....2135
- MPLS (Multiprotocol Label Switching)
  - connections, checking.....1492
  - LSPs.....1402
  - monitoring interfaces.....1402
  - monitoring LSP information.....1402
  - monitoring LSP statistics.....1403
  - monitoring MPLS interfaces.....1401
  - monitoring RSVP interfaces.....1405
  - monitoring RSVP sessions.....1404
  - monitoring traffic engineering.....1401
- mpls statement.....1584
- MPLS, monitoring.....638
- MSDP
  - supported software standards.....2143
- mtrace monitor command.....1486, 1621
  - results.....1486
- mtrace-from-source command.....1358
  - options.....1358
  - results.....1359
- multicast
  - trace operations, displaying.....1486
  - tracing paths.....1358
- Multicast MIB.....1809, 1810, 1818
- multicast-client statement.....1111
- multilink bundles
  - reducing latency.....1536
  - removing jitter.....1536
- multiple devices
  - deploying See autoinstallation
- Multiprotocol Label Switching See MPLS
- N**
  - name statement.....2042
    - usage guidelines.....1901
  - names
    - wildcard .....475
  - naming conventions, interface.....422
  - naming conventions, software.....126
  - NAT
    - supported software standards.....2156
  - NAT (Network Address Translation)
    - monitoring.....642
  - NAT Objects MIB.....1823, 1828, 1834, 1840
  - neighbor discovery
    - supported software standards.....2143
  - neighbor-discovery-router-advertisement
    - statement.....1112
  - neighbors, BGP See BGP neighbors; BGP RPM
  - probes
  - nested configuration groups.....460
  - network address translation.....29
  - Network Address Translation See NAT

Network Address Translation Objects MIB See NAT Objects MIB	
network connectivity.....	653
network interfaces	
alarm conditions and configuration	
options.....	1312
configuring alarms on.....	1316
integrated services, alarm conditions and configuration options.....	1312
monitoring.....	1395, 1400
monitoring MPLS traffic engineering.....	1402
monitoring traffic.....	1523
monitoring, CoS.....	1387
monitoring, PPPoE.....	1407
monitoring, RSVP.....	1405
packet capture, configuring on.....	1514
packet capture, disabling before changing encapsulation.....	1522
packet capture, supported on.....	1509
services, alarm conditions and configuration options.....	1312
statistics.....	1395
network management	
supported software standards.....	2115
network performance See RPM	
network.conf file, default for	
autoinstallation.....	152, 154
next hop, displaying.....	1425
no-cmd-attribute-value statement.....	1143
no-more command.....	548, 549
no-more filter.....	443
no-world-readable statement	
archiving of all system log files.....	1754
system logging.....	1780
nonpersistent statement.....	1585
accounting	
usage guidelines.....	1293
Nontemporary Address	
configuring.....	962
Nontemporary Addresses and Prefix	
Delegation.....	962
nonvolatile statement.....	2043
notice logging severity.....	632
notify statement.....	2044
usage guidelines.....	1937
notify-filter statement	
for applying to target.....	2044
usage guidelines.....	1942
for configuring.....	2045
usage guidelines.....	1915
notify-view statement.....	2045
usage guidelines.....	1930
NTP	
listening	
for broadcast messages.....	1070
supported software standards.....	2125
ntp server.....	18
NTP server, defining (Quick Configuration).....	610
ntp statement.....	1113
<b>O</b>	
object-names statement.....	1585
objects-names statement	
for Routing Engine profiles	
usage guidelines.....	1308
oid statement	
SNMP.....	2046
usage guidelines.....	1906
SNMPv3.....	2046
usage guidelines.....	1915
OK button.....	615
J-Web configuration editor.....	590
Open Shortest Path First See OSPF	
openssl command.....	605, 866
operation statement.....	1586
for MIB profiles	
usage guidelines.....	1308
operational mode, CLI	
command history.....	331
switching to configuration mode.....	311
users, monitoring.....	421
word history.....	331
operational mode, filtering command output.....	1283
operator login class permissions.....	663
operators	
arithmetic, binary, and relational	
operators.....	1527
logical.....	1526
operators, regular expression	
system logging.....	1729
option buttons	
Delete Configuration Below This Point.....	616
Discard All Changes.....	616
Discard Changes Below This Point.....	616

- 
- OSPF
    - supported software standards.....2151
  - OSPF (Open Shortest Path First)
    - monitoring.....1426
    - statistics.....1427
  - OSPF interfaces
    - displaying.....1427
    - status.....1427
  - OSPF MIB.....1806
  - OSPF neighbors
    - displaying.....1427
    - status.....1427
  - OSPF routing information.....1426
  - OSPFv3
    - supported software standards.....2151
  - outbound SSH service
    - configuring.....900
  - outbound time See RPM probes
  - outbound-ssh statement
    - usage guidelines.....900
  - overrides statement
    - DHCP local server.....1116
  - overview
    - branch SRX.....3
  - P**
  - P2MP LSPs, testing.....1637
  - packet capture.....656
    - configuring.....1514
    - configuring (J-Web).....1527
    - configuring on an interface.....1514
    - device interfaces supported.....1509
    - disabling.....1521
    - disabling before changing encapsulation on
      - interfaces.....1522
    - displaying configurations.....1512
    - displaying firewall filter for.....1517
    - enabling.....1511
    - encapsulation on interfaces, disabling before
      - modifying.....1522
    - files See packet capture files
    - firewall filters, configuring.....1516
    - firewall filters, overview.....1510
    - J-Web tool.....1527
    - overview.....1509
    - overview (J-Web).....1527
    - preparation.....1511
    - verifying captured packets.....1512
    - verifying configuration.....1512
    - verifying firewall filter for.....1517
  - packet capture configuration
    - datapath debugging.....1518
  - packet capture files
    - analyzing.....1510
    - libpcap format.....1512
    - overview.....1510
    - renaming before modifying encapsulation on
      - interfaces.....1522
  - Packet Capture page
    - field summary.....1528
    - results.....1531
  - packet encapsulation
    - troubleshooting on the link services
      - interface.....1536
    - verifying on the link services interface.....1539
  - packet filtering
    - supported software standards.....2139
  - Packet Forwarding Engine
    - MIB.....1823, 1829, 1834, 1840
  - packet fragmentation
    - troubleshooting on the link services
      - interface.....1536
    - verifying on the link services interface.....1538
  - packet headers, transmitted, displaying.....1611
  - packet loss priority, CoS.....1392
  - packet-capture statement.....1587
  - packet-filter statement
    - security.....1588
  - packets
    - capturing.....1509
    - capturing with J-Web packet capture.....1527
    - monitoring jitter.....1340
    - monitoring packet loss.....1340
    - monitoring round-trip times.....1340
    - multicast, tracking .....1358
    - packet capture.....1509
    - packet capture (J-Web).....1527
    - tracking MPLS.....1502
    - tracking with J-Web traceroute.....1486
  - pages, layout in J-Web.....587
  - parameters statement.....2047
    - usage guidelines.....1941
  - parentheses, in syntax descriptions.....lv
  - partial command entry, completing.....522
  - password retry limits, setting.....889



passwords	
for downloading software upgrades.....	141
local password method for user authentication.....	862
<i>See also</i> local password	
RADIUS.....	851
retry limits.....	889
setting login retry limits.....	889
srx root password, recovering.....	1532
paste command	
usage guidelines.....	337
PC <i>See</i> management device	
PCAP <i>See</i> packet capture	
peer entities.....	472
peer statement.....	1117
peers, BGP <i>See</i> BGP neighbors; BGP RPM probes	
performance indicators.....	1997
performance, monitoring <i>See</i> RPM	
permission bits, for login classes.....	664
permission flags	
login class.....	669
user.....	669
permissions	
denying and allowing commands.....	666
predefined.....	663
permissions statement	
usage guidelines.....	669
permissions, CLI, displaying.....	534, 1233
pfe (system logging facility).....	1718
PGM	
supported software standards.....	2143
physical interfaces, CoS.....	1387
PIC combinations	
verifying during Junos OS installation.....	137
PIM	
supported software standards.....	2143
PIMs (Physical Interface Modules)	
checking power and heat status.....	1452
ping	
host.....	653
host reachability (CLI).....	1494
host reachability (J-Web).....	1496
ICMP probes.....	1325
MPLS.....	655
RPM probes <i>See</i> RPM probes	
TCP and UDP probes.....	1329
ping command.....	1494
DHCP server operation.....	934
DHCP server operation, explanation.....	934
options.....	1494
Ping end point of LSP	
description.....	1492
using.....	1500
ping host	
results.....	658
sample.....	657
Ping Host page	
field summary.....	1497
Ping LDP-signaled LSP	
description.....	1492
using.....	1500
Ping LSP for a Layer 2 VPN connection by interface.....	655
Ping LSP to a Layer 2 circuit remote site by VCI.....	655
Ping LSP to Layer 3 VPN prefix	
description.....	1492
using.....	1500
Ping MIB.....	1823, 1829, 1834, 1840
use in ping test.....	1962
view configuration example	
SNMP.....	1907
ping MPLS	
layer-2 VPN, instance.....	655
layer-2 VPN, interface.....	655
LDP-signaled LSP.....	655
LSP endpoint.....	655
LSP to Layer 3 VPN prefix.....	655
options.....	612
RSVP-signaled LSP.....	655
ping MPLS (J-Web)	
indications.....	1502
Layer 2 circuits.....	1492
Layer 2 VPNs.....	1492
Layer 3 VPNs.....	1492
LSP state.....	1492
options.....	1492
requirements.....	1494
results.....	1502
ping mpls l2circuit command.....	1503, 1623
results.....	1502
ping mpls l2vpn command.....	1504, 1626
results.....	1502
ping mpls l3vpn command.....	1506, 1629
results.....	1502



- ping mpls ldp command.....1507, 1632
  - results.....1502
- ping mpls lsp-end-point command.....1507, 1635
  - results.....1502
- Ping MPLS page
  - field summary.....1500
  - results.....1502
- ping mpls rsvp command.....1507, 1637
  - results.....1502
- Ping RSVP-signaled LSP
  - description.....1492
  - using.....1500
- pingProbeHistoryTable.....1967
- pipe ( | )
  - command output, filtering.....439, 548
- pipe (I) command, to filter output.....1283
- Point-to-Point Protocol *See* PPP
- Point-to-Point Protocol over Ethernet *See* PPPoE
- policers, displaying.....102
- Policy Objects MIB.....1824, 1829, 1834, 1840
- policy options, configuration summary.....594
- port settings.....5
- port statement.....1768
  - SNMPv3.....2047
    - usage guidelines.....1940
  - TACACS+
    - usage guidelines.....857
  - usage guidelines.....851
- ports
  - alarm conditions and configuration
    - options.....1312
  - configuring alarms on.....1316
  - console port, securing.....888
  - DHCP interface restrictions.....922
  - individual port types.....1312
  - monitoring.....1400
  - RADIUS servers.....851
- power management, chassis.....1452
- PPP (Point-to-Point Protocol)
  - monitoring (CLI).....1406
- PPP encapsulation
  - on the link services interface.....1539
- PPP interfaces
  - supported software standards.....2128
- PPP MIB.....1806
- PPPoE (Point-to-Point Protocol over Ethernet)
  - interfaces.....1407
  - monitoring.....1407
  - session status.....1407
  - statistics.....1407
  - version information.....1407
- predefined profiles.....37
- prefix list
  - adding to SNMP community.....1944
- prefix statement.....1118
- Primary-level entry
  - secondary-level entry.....965, 1479
- Primary-level entry only.....965, 1479
- priorities
  - system logging, including in log message
    - for single-chassis system.....1725
- privacy-3des statement.....2048
  - usage guidelines.....1926
- privacy-aes128 statement.....2049
  - usage guidelines.....1925
- privacy-des statement.....2050
  - usage guidelines.....1925
- privacy-none statement.....2050
  - usage guidelines.....1926
- privacy-password statement.....2051
  - usage guidelines
    - for 3DES algorithm.....1926
    - for AES algorithm.....1925
    - for DES algorithm.....1925
- probe loss
  - monitoring.....1340
  - threshold, setting.....1337
- probe statement
  - RPM.....1589
- probe-interval statement.....1590
- probe-limit statement.....1590
- probe-server statement.....1591
- probe-type statement.....1592
- probes, monitoring.....1340, 1407
  - See also* RPM probes
- Process Details
  - monitoring.....645
- processes
  - managing.....429
  - restarting.....552, 1224
- profiles, accounting
  - filter.....1297
  - interface.....1295
  - MIB.....1307
  - Routing Engine.....1308
- programs
  - managing.....429

prompt		
setting to display in CLI.....	525	
to restart.....	526	
prompt strings		
CLI.....	484	
protect command.....	503	
usage guidelines.....	404	
protecting configuration		
usage guidelines.....	404	
protocols		
DHCP See DHCP		
originating, displaying.....	1425	
OSPF, monitoring.....	1426	
PPP, monitoring.....	1406	
RIP, monitoring.....	1425	
routing protocols, monitoring.....	1423, 1428	
<b>Q</b>		
Quick Configuration		
basic settings.....	609	
initial configuration.....	609	
RPM pages.....	1325	
quit command.....	414, 504	
usage guidelines.....	337	
<b>R</b>		
RADIUS		
authentication (configuration editor).....	855	
order of user authentication (configuration editor).....	862	
secret (configuration editor).....	855	
specifying for authentication .....	862	
supported software standards.....	2124	
RADIUS accounting.....	983	
RADIUS authentication.....	851	
security configuration example.....	851	
RADIUS authorization See RADIUS authentication		
radius-server statement		
usage guidelines.....	851	
random early detection (RED) drop profiles,		
CoS.....	1390	
rapid commit.....	964	
rapid-commit statement.....	1123	
RARP, for autoinstallation.....	154	
rate-cap statement.....	1768	
re-generate-keypair.....	1755	
re0 configuration group.....	457	
re1 configuration group.....	457	
read-only login class permissions.....	663	
read-view statement.....	2052	
usage guidelines.....	1930	
real-time monitoring		
files.....	1607, 1785	
traffic.....	1611	
real-time performance monitoring See RPM		
reboot immediately .....	627	
reconfigure statement		
DHCP local server.....	1124	
recovery software installation.....	134	
red asterisk (*).....	588	
RED drop profiles, CoS.....	1390	
redrawing screen.....	448	
redundancy-group statement.....	1593	
redundant Ethernet interface LAG.....	1348	
Refresh button.....	615	
regional configurations.....	474	
registration form, for software upgrades.....	171	
regular expression operators		
system logging.....	1729	
regular expressions		
first match, displaying from.....	442	
matching output, displaying.....	443	
nonmatching output, ignoring.....	441	
regular expressions for filtering events.....	634	
relational operators, for multicast traffic.....	1527	
relative option.....	399	
release names.....	128	
remote accounts		
accessing with SSH (CLI).....	899	
accessing with Telnet (CLI).....	898	
remote template accounts.....	677	
remote connection to router		
connecting USB modem to router.....	875	
remote operations MIBs.....	1961	
remote server, upgrading from.....	175	
remote template accounts.....	677	
remote-engine statement.....	2053	
removing		
files.....	1184	
rename command.....	505	
usage guidelines.....	351	
renaming files.....	1186	
renaming identifiers.....	351	
replace command.....	506	
usage guidelines.....	451	
replace option.....	399	
req-option statement.....	1125	

- request command.....550
  - usage guidelines.....414
- request interface modem reset umd0
  - command.....887
- request message filter.....443
- request pppoe connect command.....1642
- request pppoe disconnect command.....1643
- request security idp security-package download
  - command.....268, 271
- request support information command.....1208
- request system autorecovery state
  - command.....260, 1190
- request system configuration rescue delete
  - command.....394, 403
- request system configuration rescue save
  - command.....394, 403
- request system download abort
  - command.....262, 1192
- request system download clear
  - command.....263, 1193
- request system download pause
  - command.....264, 1194
- request system download resume
  - command.....265, 1195
- request system download start
  - command.....266, 1196
- request system firmware upgrade
  - command.....267, 1197
- request system halt command.....433
- request system license add command.....210, 1003
- request system license add terminal
  - command.....210, 1003
- request system license delete
  - command.....213, 1006
- request system license save command.....210, 1002
- request system license update
  - command.....90, 210, 270, 1003, 1198
- request system logout pid pid\_number
  - command.....344
- request system power-off fpc command.....1199
- request system reboot command.....433
- request system services dhcp command.....1200
- request system set-encryption-key algorithm des
  - command.....978
- request system set-encryption-key
  - command.....978
- request system set-encryption-key des
  - unique.....978
- request system set-encryption-key unique.....978
- request system snapshot.....134, 273, 1201
- request system software abort in-service-upgrade
  - command.....276, 1204
- request system software add .....277, 1205
- request system software reboot.....278, 1206
- request system software rollback.....134, 279, 1207
- request system storage cleanup command.....981
- request system storage cleanup dry-run
  - command.....981
- request-type statement.....2054
  - RMON
    - usage guidelines.....1989
- required entry .....588
- rescue configuration file
  - saving.....186
- rescue configuration, alarm about.....1315
- resolve command.....548
- Resource Reservation Protocol See RSVP
- restart command.....552, 1224
  - usage guidelines.....414
- restart routing command.....432
- restarting
  - after software upgrade.....484, 526
  - software processes.....552, 1224
- restoring a saved router configuration.....187
- reth
  - link aggregation group.....1348
- retransmission-attempt statement.....1126
- retransmission-interval (dhcp-client)
  - statement.....1127
- retry limits for passwords.....889
- retry statement
  - usage guidelines.....851
- retry-count statement.....2054
  - usage guidelines.....1948
- retry-interval statement.....1594
- Reverse Address Resolution Protocol (RARP), for
  - autoinstallation.....154
- Reverse-Path-Forwarding
  - MIB.....1824, 1829, 1834, 1840
- reverting to a previous configuration file
  - (J-Web).....178
- rewrite rules, CoS.....1391
- RFC 5187, OSPFv3 Graceful Restart.....2152
- RFC 5340, OSPF for IPv6.....2147, 2151
- RFC 6388, Label Distribution Protocol Extensions
  - for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths.....2135

RFCs supported See Index of Supported Software Standards	
RIP	
supported software standards.....	2153
RIP (Routing Information Protocol)	
monitoring.....	1425
statistics.....	1426
RIP neighbors	
displaying.....	1426
status.....	1426
RIP routing information.....	1425
RIPng	
supported software standards.....	2153
rising-event-index statement.....	2055
usage guidelines.....	1988
rising-threshold statement	
health monitor.....	2056
RMON.....	2055
RMON alarm entries.....	1987
RMON alarms.....	1984, 1995
RMON event entries.....	1991
RMON events.....	1985, 1994
RMON Events and Alarms	
MIB.....	1824, 1829, 1835, 1840
rmon statement.....	2056
usage guidelines.....	1994
roles	
example.....	682
rollback command.....	322, 507
usage guidelines.....	337
rolling back a configuration file during	
configuration.....	622
rolling back a configuration file, to downgrade	
software (CLI).....	178
root login to the console, disabling.....	888
root password recovery.....	1532
root password, defining (Quick Configuration).....	610
rotating files.....	980
round-trip time	
description.....	1323
See also RPM probes	
threshold, setting.....	1337
route information sample task.....	647
router.conf file, for autoinstallation.....	152
routers	
boot sequence.....	129
ports	
RADIUS servers.....	851
routes, displaying	
to specified network host.....	1712
routing	
monitoring.....	640, 1423
traceroute (J-Web).....	1486
Routing Engine profile.....	1308
Routing Engine traffic from trusted sources	
stateless firewall filters	
blocking Telnet and SSH access.....	893
Routing Engines	
synchronizing configuration.....	410
routing instances	
access lists	
configuring.....	1959
SNMP	
enabling access.....	1956
identifying.....	1955
specifying.....	1956
routing instances, configuration summary.....	595
routing options, configuration summary.....	595
routing protocols	
configuration summary.....	594
routing solutions	
applying CoS components on link services	
interface.....	1534
load balancing on link services	
interfaces.....	1536
reducing jitter and latency on multilink	
bundles.....	1536
routing table	
monitoring.....	1423
routing, monitoring.....	640, 1423
routing-engine-profile statement.....	1595
usage guidelines.....	1308
routing-instance statement	
SNMP.....	2059
SNMPv3.....	2060
usage guidelines.....	1940
usage guidelines.....	851
routing-instance-access.....	2060
RPC	
displaying command output in.....	441
RPM	
supported software standards.....	2156
RPM (real-time performance monitoring)	
basic probes (configuration editor).....	1325
BGP monitoring See BGP RPM probes	
graph results.....	640
inbound and outbound times.....	1323

- jitter, viewing.....1340
  - monitoring.....639
  - monitoring probes.....1340
  - overview.....1321
    - See also RPM probes
  - preparation.....1325
  - probe and test intervals.....1322
  - probe counts.....1323
  - Quick Configuration.....1325
  - round-trip times, description.....1323
  - round-trip times, viewing.....1340
  - RPM probes.....640
  - sample configuration.....1328
  - sample graphs.....640, 1340
  - statistics.....1323
  - statistics, verifying.....1328
  - TCP probes (configuration editor).....1329
    - See also TCP RPM probes
  - tests.....1322
  - tests, viewing.....1340
  - threshold values.....1324
  - tuning probes.....1336
  - UDP probes (configuration editor).....1329
    - See also UDP RPM probes
  - verifying probe servers.....1331
  - RPM pages.....1325
    - field summary.....1337
  - RPM probe timestamps
    - overview.....1322
    - setting (configuration editor).....1325
  - RPM probes
    - basic (configuration editor).....1325
    - BGP neighbors See BGP RPM probes
    - cumulative jitter.....1340
    - current tests.....1340
    - DSCP bits (Quick Configuration).....1337
    - graph results.....1340
    - ICMP (configuration editor).....1325
    - inbound times.....1323
    - jitter threshold.....1337
    - monitoring.....1340
    - outbound times.....1323
    - probe count, setting (Quick Configuration).....1337
    - probe count, tuning.....1336
    - probe counts.....1323
    - probe intervals.....1322
    - probe intervals, setting (Quick Configuration).....1337
    - probe intervals, tuning.....1336
    - probe loss count.....1337
    - probe owner.....1337
    - probe type, setting (Quick Configuration).....1337
    - probe types.....1321
    - round-trip time threshold.....1337
    - round-trip times, description.....1323
    - round-trip times, viewing.....1340
    - SNMP traps (Quick Configuration).....1337
    - source address, setting.....1336
    - TCP (configuration editor).....1329
      - See also TCP RPM probes
    - TCP server port.....1337
    - test intervals.....1322
    - test intervals, setting (Quick Configuration).....1337
    - test target.....1337
    - threshold values, description.....1324
    - threshold values, setting (Quick Configuration).....1337
    - timestamps See RPM probe timestamps
    - tuning.....1336
    - UDP (configuration editor).....1329
      - See also UDP RPM probes
    - UDP server port.....1337
    - verifying TCP and UDP probe servers.....1331
  - RSVP
    - LSP connections
      - operability, checking.....1637
      - supported software standards.....2137
  - RSVP (Resource Reservation Protocol)
    - interfaces, monitoring.....1405
    - sessions, monitoring.....1404
  - RSVP LSPs
    - ping interval.....1637
  - RTT See RPM probes, round-trip times
  - run command.....508
    - usage guidelines.....337
- ## S
- sample configuration
    - for secure access.....871
    - for SSL certificates.....871
  - sample tasks
    - configuring accounting options.....616
    - filtering and viewing events.....635
    - managing snapshots.....626
    - monitoring interfaces.....645

monitoring route information.....	647	JUNOScript SSL access.....	606
ping host.....	657	overview.....	865
viewing alarms.....	629	requirements.....	866
sample-type statement.....	2061	sample configuration.....	871
usage guidelines		verifying secure access configuration.....	871
for alarms.....	1990	Secure Access page	
for events.....	1991	description.....	606
samples		field summary.....	607
alarm configuration.....	1318	Secure Sockets Layer See SSL	
basic RPM probes.....	1325	security	
local template account.....	677	access privileges.....	663, 674
RPM probes.....	1328	alarms.....	1692
RPM test graphs.....	1340	console port security.....	888
TCP and UDP probes.....	1329	log.....	1782
user account.....	674	log file.....	1784
SAP		NAT.....	29
supported software standards.....	2143	packet capture for intrusion detection.....	1509
save command.....	509, 548	password retry limits.....	889
usage guidelines.....	337, 394	policies.....	23
saving licenses (CLI).....	210, 1002	configuration.....	24
saving rescue configuration file.....	186	user accounts.....	667, 674
scheduler maps, CoS.....	1392	user authentication.....	673
scheduling a reboot.....	627	zones.....	23
screen		configuration.....	24
dimensions.....	483, 486	Security Configuration Statement Hierarchy.....	57
redrawing.....	448	Security Interface Extension Objects	
screen length, setting.....	527	MIB.....	1824, 1829, 1835, 1841
screen width, setting.....	528	security log file	
SDH		binary format.....	1746
supported software standards.....	2129	security logs.....	1749
SDP		streaming through revenue ports.....	1749
supported software standards.....	2143	security policy	
secret		DNS name resolution.....	1533
RADIUS (configuration editor).....	855	Security Screening Objects MIB.....	1824, 1835, 1841
TACACS+ (configuration editor).....	859	security, configuration summary.....	595
secret statement		security-level statement	
authentication		for access privileges.....	2062
usage guidelines, RADIUS.....	851	usage guidelines.....	1928
usage guidelines, TACACS+.....	857	for SNMP notifications.....	2063
secure access		usage guidelines.....	1943
establishing.....	865	security-log-percent-full	
generating SSL certificates.....	605, 866	security alarms.....	1770
HTTPS access.....	606, 868	security-model statement	
HTTPS access (configuration editor).....	869	for access privileges.....	2064
HTTPS recommended.....	605, 865	usage guidelines.....	1928
installing SSL certificates.....	606, 868	for groups.....	2065
installing SSL certificates (configuration		usage guidelines.....	1932
editor).....	869	for SNMP notifications.....	2065
Junos XML protocol SSL access.....	868	usage guidelines.....	1943

- 
- security-name statement
    - for community string.....2066
    - for security group.....2067
      - usage guidelines.....1932
    - for SNMP notifications.....2068
      - usage guidelines.....1943
  - security-to-group statement.....2069
    - usage guidelines.....1926
  - serial cable, disconnection for console logout.....888
  - serial interfaces
    - supported software standards.....2130
  - Serial Line Address Resolution Protocol (SLARP),
    - for autoinstallation.....154
  - serial ports
    - alarm conditions and configuration
      - options.....1312
    - autoinstallation on.....152
    - configuring alarms on.....1316
  - Series
    - user interfaces *See* user interfaces
  - server address statement.....1131
  - server statement
    - NTP.....1130
  - service quality
    - monitoring.....1996
  - service sets, monitoring.....643
  - service-name statement.....1143
  - Services Gateway
    - licenses.....196, 989
    - user interfaces *See* user interfaces
  - services module
    - alarm conditions and configuration
      - options.....1312
  - Services Router
    - as a DHCP server.....920
    - licenses.....196, 989
    - monitoring .....1283
    - performance monitoring.....1321
    - user interfaces *See* user interfaces
  - services statement
    - remote router access.....1132
  - services, configuration summary.....595
  - sessions
    - BGP peer, status details.....1429
    - limiting number of.....649
    - limits.....649
    - RSVP, monitoring.....1404
    - Telnet.....898
    - terminating.....649
  - sessions, J-Web.....586
  - set cli complete-on-space command.....522
    - usage guidelines.....485
  - set cli directory command.....523
    - usage guidelines.....484
  - set cli idle-timeout command.....524
    - usage guidelines.....484
  - set cli prompt command.....525
    - usage guidelines.....484
  - set cli restart-on-upgrade command.....526
    - usage guidelines.....484
  - set cli screen-length command.....527
    - usage guidelines.....483, 486
  - set cli screen-width command.....528
  - set cli terminal command.....529
    - usage guidelines.....484
  - set cli timestamp command.....530
    - usage guidelines.....484
  - set command.....346
    - configuration mode.....511, 562
    - usage guidelines.....337
  - set date command.....531
  - set no-encrypt-configuration-files command.....978
  - set option.....400
  - Set requests, SNMP.....1800
  - Set Up page
    - field summary.....610
    - prerequisites.....609
  - setup
    - Quick Configuration.....609
    - requirements.....609
  - severity
    - security log.....1770
  - severity levels
    - for alarms *See* alarm severity
  - severity levels for events.....632
  - SHA-1 (Secure Hash Algorithm) checksum.....127
  - sha-256 checksum, calculating.....1178
  - SHA-1 checksum, calculating.....1177
  - show bgp neighbor command.....1428
  - show bgp summary command.....1428
  - show chassis alarms command.....1318, 1645
  - show chassis cluster ip-monitoring status
    - redundancy-group command.....1650
  - show chassis environment command.....1452
  - show chassis hardware command.....1450, 1452
  - show chassis power-ratings command.....1452
  - show chassis redundant-power-supply
    - command.....1452



show chassis routing-engine bios.....	147	show ppp statistics command.....	1406
show chassis routing-engine		show ppp summary command.....	1406
command.....	1230, 1452	show pppoe interfaces command.....	1407, 1687
show chassis usb storage command.....	280	show pppoe statistics command.....	1407, 1690
show class-of-service classifier		show pppoe version command.....	1407
command.....	1388, 1393	show redundant-power-supply command.....	1452
show class-of-service code-point-aliases		show rip neighbors command.....	1425
command.....	1389	show rip statistics command.....	1425
show class-of-service drop-profile		show route detail command.....	1423
command.....	1390	show route terse command.....	1423
show class-of-service forwarding-class		show security alarms command.....	1692
command.....	1390	show security datapath-debug capture.....	1696
show class-of-service rewrite-rules		show security datapath-debug counter.....	1697
command.....	1391	show security flow session command.....	91
show class-of-service scheduler-map		show security idp active-policy command.....	97
command.....	1392	show security idp status command.....	98
show cli authorization command.....	534, 1233	show security log command.....	1791
show cli command.....	532	show security log file command.....	1794
usage guidelines.....	485	show security monitoring fpc fpc-number	
show cli directory command.....	535	command.....	1698
show cli history command.....	536	show security nat destination summary	
usage guidelines.....	331	command.....	100
show command		show security policies command.....	102
configuration mode.....	563	show security utm session.....	110
usage guidelines.....	337	show security utm status.....	111
show configuration command.....	564, 1647	show security zones command.....	112
show dhcpv6 server binding.....	1251	show services ip-monitoring status	
show dhcpv6 server statistics command.....	1255	command.....	1703
show firewall command.....	1258	show services rpm active-servers	
show firewall filter dest-all command.....	1517	command.....	1331, 1334
show groups junos-defaults command.....	571	explanation.....	1331, 1334
usage guidelines.....	481	show services rpm probe-results	
show interfaces command.....	1653	command.....	1328, 1340, 1707
show interfaces detail command.....	1400	explanation.....	1328
show interfaces dlo extensive command.....	882	show snmp mib command.....	2102
show interfaces interface-name command.....	1400	show system alarms command.....	1711
show interfaces pp0 command.....	1407	show system auto-snapshot command.....	281
show interfaces terse command.....	1400	show system autoinstallation status	
show log command.....	1744, 1789	command.....	156
show mpls interface command.....	1401	show system autorecovery state	
show mpls lsp command.....	1402	command.....	283, 1260
show mpls statistics command.....	1403	show system commit command.....	572
show ospf interfaces command.....	1426	show system download command.....	285, 1264
show ospf neighbors command.....	1426	show system license	
show ospf statistics command.....	1426	command.....	115, 212, 214, 287, 1005, 1007, 1266
show poe interface command.....	1683	explanation.....	212, 214, 1005, 1007
show poe telemetries.....	1685	show system license keys command.....	213, 1006
show ppp address-pool command.....	1406	show system license usage command.....	213, 1005
show ppp interface command.....	1406	explanation.....	213, 1005



- 
- show system log-vital command.....2105
  - show system login lockout command.....1269
  - show system processes command.....1744
  - show system processes extensive command.....430
    - output, table.....431
  - show system services dhcp binding
    - command.....933
  - show system services dhcp binding detail
    - command.....933
  - show system services dhcp client
    - command.....118, 941, 974, 1270
  - show system services dhcp client interface
    - command.....941, 974
  - show system services dhcp client statistics
    - command.....942
  - show system services dhcp conflict
    - command.....922
  - show system services dhcp global command.....933
  - show system services dhcp relay-statistics
    - command.....948, 1273
    - explanation.....948
  - show system snapshot media.....183, 290, 1275
  - show system statistics command.....572
  - show system storage command.....1450
  - show system storage
    - partitions.....291, 293, 1276, 1278
  - show system uptime command.....1450
  - show system users command.....1450
  - show version.....138
  - show version command.....138, 1450
    - Junos OS.....428
  - show | display inheritance command.....567
  - show | display inheritance defaults command
    - usage guidelines.....481
  - show | display omit command.....568
  - show | display set command.....569
    - usage guidelines.....367
  - show | display set relative.....570
  - show | display set relative command.....570
    - usage guidelines.....368
  - show forwarding-options command.....1512
  - side pane, J-Web.....589
  - single-connection statement
    - usage guidelines.....857
  - SIP
    - supported software standard.....2156
  - size statement.....1771
    - accounting.....1598
    - usage guidelines.....1293
    - archiving of all system log files.....1754
  - SLARP, for autoinstallation.....154
  - snapshot
    - sample task.....626
  - SNMP
    - adding client lists and prefix lists.....1944
    - agent.....1800, 1802
    - architecture.....1800
    - commit delay timer.....1902
    - community string.....1902
    - configuration
      - version 3.....2007
      - versions 1 and 2.....1898
    - configuration summary.....595
    - enterprise-specific traps See SNMP traps
    - filtering duplicate requests.....1904
    - limiting interface access.....1905
    - logging, enabling.....1962
    - manager.....1800
    - master agent.....1802
    - MIB object values, displaying.....2102
    - MIB views.....1906
    - remote operations.....1960
    - standard traps See SNMP traps
    - standards documents.....1804
    - subagent.....1802
    - system contact.....1900
    - system description.....1901
    - system location.....1900, 2037
    - system name.....1901
    - tracing operations.....1969
    - trap groups.....1912
    - trap notification for remote operations.....1961
    - trap options.....1909
    - views, setting.....1960
  - SNMP informs.....1935
  - snmp statement.....2069
    - usage guidelines
      - SNMPv1 and SNMPv2.....1898
      - SNMPv3.....2007
  - SNMP traps.....1801
    - enterprise-specific
      - version 1.....1869
      - version 2.....1876
    - performance monitoring See RPM probes
    - source address configuration.....1909

standard		SRX Series.....	977
version 1.....	1884	alarms.....	1310
version 2.....	1887	licenses.....	196, 989
system logging severity levels.....	1802	managing user authentication.....	673
unsupported.....	1892	monitoring .....	1283
snmp-community statement.....	2070	packet capture.....	1509
SNMPv2		performance monitoring.....	1321
MPLS traps.....	1890	system log messages.....	1744
Passive Monitoring Traps MIB.....	1912	SRX series device	
SNMPv3		bring components online/offline.....	189
authentication, configuring.....	1923	halting.....	189
informs, configuring.....	1935	rebooting.....	189
local engine ID, configuring.....	1934	SRX series devices	
minimum configuration.....	1922	software upgrades.....	169
SNMPv3 context		SRX Series Services Gateway.....	181 See storage
usage guidelines.....	1946	m          e          d          i          a	
software installation		auto bios upgrade methods.....	177
category change installation		boot devices	
description.....	134	configuring (CLI).....	181
recovery installation		configuring (J-Web).....	181
description.....	134	configuring boot devices.....	181
standard installation		dual-root partitioning.....	156
description.....	133	Install Remote page	
software installation packages		field summary.....	181
Junos OS for SRX devices, domestic		installing software	
description.....	134	with CLI.....	162
Junos OS for SRX devices, export		with J-Web.....	162
description.....	134	Junos OS Release 10.0	
software packages		upgrading without dual-root.....	169
upgrading individual.....	167	multiple devices, using snapshots to replicate	
software upgrade		configurations	
restarting after.....	526	J-Web.....	181
software, halting immediately.....	627	request system snapshot command.....	181
SONET		show system storage partitions.....	165
supported software standards.....	2129	Snapshot page.....	181
Source Class Usage MIB.....	1824, 1835, 1841	snapshots.....	181
source-address statement.....	2070	software upgrade methods.....	169
NTP.....	1137	See also boot devices	
RADIUS		SSH	
usage guidelines.....	851	accessing remote accounts (CLI).....	899
RADIUS and TACACS+.....	1137	setting login retry limits.....	889
system logging.....	1137	ssh command.....	899
usage guidelines.....	1909	options.....	899
usage guidelines, RADIUS.....	851	usage guidelines.....	414
source-classes statement.....	1598	SSH, defining access (Quick Configuration).....	612
usage guidelines.....	1305	ssh-known-hosts statement.....	1138
SPU Monitoring MIB.....	1825, 1835		
SPU monitoring MIB.....	1841		
SRC application.....	301, 578		

- 
- SSL (Secure Sockets Layer)
    - enabling secure access.....606, 868
    - management access.....865
    - verifying SSL configuration.....871
  - SSL 3.0 option, disabling on Internet Explorer for
    - worldwide version of Junos OS.....581, 604
  - SSL access, establishing.....865
  - SSL certificates
    - adding.....871
    - adding (configuration editor).....869
    - adding (Quick Configuration).....607
    - generating.....605, 866
    - sample configuration.....871
    - verifying SSL configuration.....871
  - standard software installation.....133
  - standard traps, SNMP
    - version 1.....1884
    - version 2.....1887
  - standards documents
    - SNMP and MIBs.....1804
  - start-time statement
    - accounting.....1599
    - usage guidelines.....1293
  - startup
    - J-Web interface.....581, 604
  - startup, J-Web interface.....581, 604
  - startup-alarm statement.....2071
    - usage guidelines.....1990
  - stateful firewall.....55
  - stateless firewall filters
    - examples
      - blocking Telnet and SSH access.....893
  - statistics
    - BGP.....1429
    - interfaces.....1395
    - LSP.....1403
    - OSPF.....1427
    - performance monitoring.....1323
    - PPPoE.....1407
    - RIP.....1426
    - RPM, description.....1323
    - RPM, monitoring.....1340
    - RPM, verifying.....1328
  - status
    - autoinstallation.....156
    - BGP.....1429
    - license key.....197, 990
    - OSPF interfaces.....1427
    - OSPF neighbors.....1427
    - RIP neighbors.....1426
    - status command.....512
      - usage guidelines.....337, 369
    - storing previous configurations.....389
    - streaming security logs through revenue
      - ports.....1749
    - strings
      - help about.....326
  - Structure of Management Information
    - MIB.....1825, 1826, 1831
      - Junos OS for SRX Series devices,
        - for.....1826, 1831, 1836
    - structured-data statement.....1772
      - usage guidelines.....1724
    - subagent, SNMP.....1802
    - super-user login class permissions.....663
    - superuser login class permissions.....663
    - support, technical See technical support
      - system information, displaying.....1208
    - symbol.....443
    - syntax conventions.....lv
    - sysContact object, MIB II.....1900
    - sysDescription object, MIB II.....1901
    - sysLocation object, MIB II.....1900
    - syslog See system logs
    - syslog statement
      - system processes.....1773
    - syslog-subtag statement.....2071
      - usage guidelines.....1990
    - sysName object, MIB II.....1901
    - system.....690
      - configuration summary.....595
      - login lockout.....1173, 1269
      - monitoring.....644
      - retry options.....690
    - system access and access management
      - supported software standards.....2125
    - system authentication
      - RADIUS
        - configuring.....851
      - TACACS+ .....857
  - System Configuration Statement
    - Hierarchy.....217, 1028
  - system contact, SNMP.....1900
  - system description, SNMP.....1901
  - system location, SNMP.....1900, 2037

system log messages	
/var/log directory.....	1748
capturing in a file (configuration editor).....	1748
destinations.....	1744, 1748
displaying at a terminal (configuration editor).....	634
event viewer.....	1447, 1750
filtering.....	632
monitoring (Quick Configuration).....	1750
overview.....	630, 1744
System Log MIB.....	1825, 1830, 1835, 1841
system logging	
disabling.....	1730
examples.....	1730
facilities	
default for remote machine.....	1727
for local machine.....	1718
message descriptions	
displaying.....	1735
fields in.....	1735
messages, displaying	
generated by service on PIC.....	1742
structured-data format.....	1737
regular expression filtering.....	1728
regular expression operators.....	1729
timestamp, modifying.....	1727
system logging severity levels, SNMP traps.....	1802
system logs	
control plane logs.....	1745
data plane logs.....	1745
enabling.....	652
file cleanup .....	625
file cleanup (CLI).....	981
file cleanup (J-Web).....	980
functions.....	630, 1744
logging severity levels.....	632
messages See system log messages See system log messages	
monitoring.....	1485
overview.....	1744
redundant syslog server.....	1744
remote system log server.....	1748
sending through eventd.....	1748
system management	
displaying log and trace file contents.....	1485
files.....	625
login classes.....	663, 674
reboots.....	627
system logs.....	1744
template accounts.....	677
user accounts.....	667, 674
user authentication.....	673
system name, SNMP.....	1901
system services.....	8
outbound SSH.....	900
system statement.....	1774
system time	
defining (Quick Configuration).....	611
synchronizing (Quick Configuration).....	610
<b>T</b>	
T1 ports	
alarm conditions and configuration	
options.....	1312
configuring alarms on.....	1316
T3 interfaces	
supported software standards.....	2130
T3 ports	
alarm conditions and configuration	
options.....	1312
configuring alarms on.....	1316
TACACS+	
authentication (configuration editor).....	859
order of user authentication (configuration editor).....	862
secret (configuration editor).....	859
specifying for authentication.....	862
supported software standards.....	2124
TACACS+ authentication	
configuring.....	857
tacplus.....	1142
tacplus-options statement.....	1143
usage guidelines.....	858
tacplus-server statement.....	1144
usage guidelines.....	857
tag statement.....	2072
SNMPv3	
usage guidelines.....	1947
usage guidelines.....	1937
tag-list statement.....	2072
usage guidelines.....	1940
target statement.....	1599
target-address statement.....	2073
usage guidelines.....	1939
target-parameters statement.....	2074
usage guidelines.....	1941
targets statement.....	2075
usage guidelines.....	1912

- 
- taskbar.....583, 588
  - TCP
    - supported software standards.....2145
  - TCP RPM probes
    - CoS classification, destination interface requirement.....1329
    - CoS classification, use with caution.....1329
    - description.....1321
    - server port.....1337
    - setting.....1329
    - verifying servers.....1331
  - technical support
    - contacting JTAC.....lvii
    - system information, displaying.....1208
  - Telnet
    - accessing remote accounts (CLI).....898
    - setting login retry limits.....889
  - telnet command.....898
    - options.....898
    - usage guidelines.....414
  - Telnet session.....898
  - Telnet, defining access (Quick Configuration).....611
  - template accounts
    - description.....677
    - local accounts (configuration editor).....677
    - remote accounts (configuration editor).....677
  - temporary files
    - cleaning up (CLI).....981
    - cleaning up (J-Web).....980
    - downloading (J-Web).....983
    - for packet capture.....1510
  - temporary files, cleaning up.....625
  - terminal screen
    - length, setting.....527
    - width, setting.....528
  - terminal type.....484
    - setting.....529
  - tests See RPM
  - TFTP, for autoinstallation.....152
  - threshold values, for RPM probes See RPM probes
  - thresholds statement
    - RPM.....1600
  - time synchronization
    - supported software standards.....2125
  - time to live See TTL
  - time zone, defining (Quick Configuration).....610
  - time-format statement.....1775
    - usage guidelines.....1727
  - timeout sessions.....649
  - timeout statement.....2075
    - authentication
      - usage guidelines, RADIUS.....851
      - usage guidelines, TACACS+ .....857
    - usage guidelines.....1948
  - timeout, user, setting.....524
  - timestamp, CLI output, setting.....530
  - timestamps
    - for RPM probes See RPM probe timestamps
    - suppressing in packet headers, in captured packets.....1528
    - suppressing in packet headers, in traffic monitoring.....1524
  - top command.....513
    - usage guidelines.....337, 351
  - top pane, J-Web.....587
  - trace files
    - display of
      - starting.....1608, 1786
      - stopping.....1610, 1788
    - monitoring.....1485
    - multicast, monitoring.....1486
    - status, displaying.....1607, 1785
  - traceoptions
    - security log.....1776
  - traceoptions (outbound-ssh).....1146
  - traceoptions statement.....514, 2076
    - datapath-debug.....1601
    - DHCP local server.....1148
    - SNMP
      - usage guidelines.....1969
  - traceroute
    - CLI command.....1490
    - indications.....1488
    - J-Web tool.....1486
    - results.....1488
    - TTL increments.....1486
  - traceroute command.....1490, 1712
    - options.....1490
  - Traceroute MIB.....1825, 1830, 1836, 1841, 1969
  - traceroute monitor
    - CLI command.....1360
  - traceroute monitor command.....1360
    - options.....1360
    - results.....1361
  - Traceroute page
    - field summary.....1487
  - traceroute, overview.....656

tracing.....	1778	J-Web behavior.....	651
destination-override.....	1778	jitter and latency on multilink bundles.....	1536
tracing operations		LFI and load balancing on multilink	
SNMP.....	1969	bundles.....	1536
tracing routes		packet capture for analysis.....	1509
monitoring.....	1621	<i>See also</i> diagnosis; packet capture	
traffic		root password recovery.....	1532
analyzing with packet capture.....	1509	router connectivity.....	651
multicast, tracking.....	1358	trusted-key statement.....	1150
tracking with J-Web traceroute.....	1486	TTL (time to live)	
traffic, real-time monitoring.....	1611	default, in multicast path-tracking	
transfer-interval statement		queries.....	1358
accounting.....	1602	increments, in traceroute packets.....	1486
usage guidelines.....	1294	threshold, in multicast trace results.....	1359
trap groups, SNMP.....	1912	total, in multicast trace results.....	1359
trap notification for SNMP remote		TTL (time to live), ping requests.....	658
operations.....	1961	TX Matrix router	
trap-group statement.....	2078	configuration groups.....	457
usage guidelines.....	1912	configuration groups example.....	462
trap-options statement.....	2079	type checking, CLI.....	397
usage guidelines.....	1909	type statement.....	2080
traps.....	1876	usage guidelines.....	1937
definition.....	1801		
SNMP version 1 traps		<b>U</b>	
enterprise-specific.....	1869	UDP	
standard.....	1884	supported software standards.....	2145
SNMP version 2 traps		UDP RPM probes	
enterprise-specific.....	1876	CoS classification, destination interface	
standard.....	1887	requirement.....	1329
unsupported.....	1892	CoS classification, use with caution.....	1329
<i>See also</i> SNMP traps		description.....	1321
traps statement.....	1603	server port.....	1337
trim command.....	548	setting.....	1329
Trivial File Transfer Protocol (TFTP), for		verifying servers.....	1331
autoinstallation.....	152	umd0.....	872
troubleshoot		unauthorized login class permissions.....	663
CLI terminal.....	599	unified threat management.....	37
network connectivity.....	653	UNIX operating system.....	299, 300
packet capture.....	656	UNIX shell.....	300
ping host.....	653	unknown logging severity.....	632
ping MPLS.....	655	unprotect command.....	515
traceroute.....	656	usage guidelines.....	404
troubleshoot sample task.....	657	unprotecting configuration	
troubleshooting		usage guidelines.....	404
applying CoS components on link services		unsupported standard SNMP traps.....	1892
interface.....	1534	up command.....	516
DNS name resolution in security policy.....	1533	usage guidelines.....	337, 351
events.....	652	update command.....	517
J-Web access.....	652	usage guidelines.....	337

- 
- update-router-advertisement statement.....1152
  - update-server (dhcp-client) statement.....1152
  - update-server statement.....1152
  - updating
    - licenses (CLI).....210, 1003
  - upgrade, restarting after.....484
  - upgrades
    - downloading.....141
    - installing (CLI).....173
    - installing by uploading.....173
    - installing from remote server.....175
    - requirements.....171
  - upgrading or downgrading Junos OS.....167
  - upgrading software.....484
    - prompt to restart after.....526
  - uploading a configuration file.....624
  - URLs
    - software downloads.....141
  - URLs, specifying in commands.....426
  - usb.....258
  - USB modem connections
    - connecting dial-up modem at user end.....886
    - dialer interface *See* dialer interface, USB
    - modem
    - interface naming conventions.....872
    - requirements.....875
    - USB modem interface types.....872
    - verifying dialer interfaces.....882
  - USB modem interfaces
    - dialer interface *See* dialer interface, USB
    - modem
  - USB modems
    - AT commands.....874
    - default modem initialization commands.....874
    - initialization by device.....874
    - resetting.....887
  - use-interface statement.....1153
  - user (system logging facility).....1718
  - user accounts
    - authentication order (configuration editor).....862
    - configuration example.....312
    - contents.....667
    - creating (configuration editor).....674
    - for local users.....677
    - for remote users.....677
    - predefined login classes.....663
    - templates for.....677
    - See also* template accounts
  - user interfaces
    - Junos Scope application.....301, 578
    - overview.....301, 578
    - preparation.....581, 604
    - SRC application.....301, 578
  - user permission flags.....669
  - user roles
    - example.....682
  - user statement
    - SNMPv3.....2080
    - system logging.....1779
    - usage guidelines.....1724
  - user timeout, setting.....524
  - user-id statement.....1154
  - username
    - description.....667
    - specifying .....674
  - users
    - access privileges.....663, 674
    - accounts *See* user accounts
    - adding.....674
    - CLI permissions, displaying.....534, 1233
    - editing configuration
      - displaying.....369
      - multiple simultaneous users.....375
    - login classes.....663, 674
    - logs, displaying.....1789
    - of CLI, monitoring.....421
    - predefined login classes.....663
    - template accounts *See* template accounts
    - usernames.....667
    - viewing.....649
  - using alarms tasks.....628
  - usm statement.....2081
  - Utility MIB.....1825, 1830, 1836, 1841
  - UTM.....37
    - antispam.....37
    - antivirus.....37
    - configuration.....38
    - profiles.....42
    - webfiltering.....37
  - utm-policy.....37
- V**
- v3 statement.....2083
    - usage guidelines.....2007
  - vacm statement.....2085
    - usage guidelines.....1926
  - validating software compatibility.....137



var/log/mib2d file.....	1969	view statement	
var/log/snmpd file.....	1969	SNMP (associating with community).....	2087
variable statement.....	2086	usage guidelines.....	1902
usage guidelines.....	1991	SNMP (configuring MIB view).....	2088
variable-length string indexes.....	1961	usage guidelines.....	1906
vendor-id statement.....	1154	viewing alarms, sample task.....	629
verification		viewing configuration text.....	595
active licenses.....	212, 214, 1005, 1007	viewing events, sample task.....	635
alarm configurations.....	1318	views, MIB	
autoinstallation.....	156	SNMP.....	1906, 1960
captured packets.....	1512	VLAN.....	5
destination path (J-Web).....	1486	vlan.....	6
DHCP server operation.....	934	voice calls, not supported in dial-in .....	872
DHCP statistics.....	948	voice services	
dialer interfaces.....	882	supported software standards.....	2157
firewall filter for packet capture.....	1517	VPLS	
host reachability (CLI).....	1494	supported software standards.....	2159
host reachability (J-Web).....	1496	VPN	
license usage.....	213, 1005	IPsec.....	56
licenses .....	212, 214, 1005, 1007	VPN Certificate Objects	
load balancing on the link services		MIB.....	1825, 1830, 1836, 1842
interface.....	1540	VPN MIB.....	1826
LSPs (J-Web).....	1492	vpn statement.....	1155
packet capture.....	1512	VPNs	
packet encapsulation on link services		carrier-of-carriers	
interface.....	1539	supported software standards.....	2157
RPM configuration.....	1328	interprovider	
RPM probe servers.....	1331, 1334	supported software standards.....	2157
RPM statistics.....	1328	Layer 2	
secure access.....	871	supported software standards.....	2132, 2157
tracing multicast paths.....	1358	Layer 3	
version		supported software standards.....	2158
PPPoE, information about.....	1407	multicast	
version statement		supported software standards.....	2159
SNMP.....	2086	VPNs (virtual private networks), DHCP support on	
usage guidelines.....	1912	interfaces.....	922
version, license key.....	197, 990		
view and edit		<b>W</b>	
committing a text file, with caution.....	597	WAN.....	5
configuration text, viewing.....	595	warning logging severity.....	632
configuration, editing.....	593	Web access, secure See secure access	
uploading a file.....	624	Web browser, modifying Internet Explorer for	
View Configuration Text page.....	596	worldwide version of Junos OS.....	581, 604
View Events page		Web Filtering	
field summary (filtering log		verifying.....	1466
messages).....	633, 1424	web-management statement.....	1157
overview.....	630	wildcard characters.....	465
		wildcard command.....	519



wildcard delete command	
usage guidelines.....	455
wildcard names.....	475
wildcard range command	
usage guidelines.....	354
windows, J-Web, unpredictable results with	
multiple.....	586, 651
word history	
operational mode.....	331
working directory	
current, setting.....	523
displaying.....	535
world-readable statement	
archiving of all system log files.....	1754
system logging.....	1780
write-view statement.....	2089
usage guidelines.....	1930
 <b>X</b>	
XML format	
displaying command output in.....	441
 <b>Y</b>	
yellow alarms.....	629, 1311 See minor alarms

